- **Procedimiento Nº: PS/00029/2020**

938-300320

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 25 de septiembre de 2019 la directora de la Agencia Española de Protección de Datos (en adelante AEPD) acuerda iniciar actuaciones de investigación en relación a una violación de seguridad de datos personales (en adelante Brecha de Seguridad) notificada por el SERVICIO DE SALUD DE CASTILLA-LA MANCHA, con NIF Q4500146H, relativa a la pérdida de datos y accesos indebidos al historial de pacientes en diferentes hospitales de la citada Comunidad Autónoma.

El SESCAM ha notificado a esta Agencia los siguientes hechos:

"El servicio de "X" del hospital de "Y" ha consultado un documento archivado de un paciente del propio hospital y se le ha mostrado la documentación de un paciente del hospital de "Z". No se configuró correctamente la ruta donde se almacenan los archivos de cada paciente, compartiéndose la misma ubicación para distintos hospitales. La identificación de los distintos archivos se realizaba mediante una secuencia numérica. Estos aspectos provocaron la sustitución de ficheros con el mismo nombre de distintos pacientes y la aparición de documentos cruzados entre distintos hospitales."

Informan de que la brecha de seguridad afecta a la confidencialidad, integridad y disponibilidad de los datos básicos y de salud de unos 431 pacientes.

SEGUNDO: A la vista de los hechos notificados y de los documentos aportados por el responsable del tratamiento, la Subdirección General de Inspección de Datos inicia actuaciones previas de investigación para el esclarecimiento de los hechos notificados por el SESCAM, en virtud de los poderes de investigación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad: 16/09/2019

ENTIDAD INVESTIGADA

SERVICIO DE SALUD DE CASTILLA LA MANCHA (en adelante SESCAM), con NIF Q4500146H y con domicilio en la Avenida Río Guadiana 4, 45071 - Toledo (Toledo)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto a los hechos.

- Se ha producido un solapamiento de ficheros adjuntos dentro de la aplicación VITROPATH (**VITROPATH** es un **sistema integrado** para la **gestión del servicio de Anatomía Patológica)** por los usuarios de la aplicación en cuatro Hospitales del SESCAM.

  Destacan que la información indebidamente indexada sólo corresponde a los ficheros adjuntos al informe realizado por el Servicio de Patología. En ningún caso se ha desindexado el informe realizado tomando como base el fichero adjunto, con lo que la información suministrada a médicos y pacientes no está comprometida dado que el fichero adjunto sólo se consulta desde el propio Servicio de Anatomía Patológica.

  Hay 423 ficheros que no se han podido recuperar. Se ha puesto en conocimiento de los servicios de Anatomía Patológica de los centros afectados para que analicen la posibilidad de recuperar la información de copias en papel.

- La cronología de los hechos es la siguiente:

  El 09/09/2019 a las 12:50 se recibe en el Soporte de Imagen Médica una llamada de VITROPATH comunicando que les había llegado una incidencia indicando que desde el Hospital de Puertollano estaban consultando documentos adjuntos en VITROPATH y aparecían documentos de otro Hospital.

  Esta incidencia fue comunicada por la Jefa de Servicio de uno de los Hospitales adscritos al SESCAM directamente al proveedor de VITROPATH por correo electrónico en vez de comunicarla por el sistema de registro de incidencias IRIS tal como está protocolizado.

  La incidencia llega al SESCAM por comunicación telefónica del proveedor al grupo de Soporte Imagen Médica. Tras analizar el problema por el grupo de Soporte Imagen Médica junto con soporte Middleware se descubrió que en los despliegues de VITROPATH no se había configurado la ruta donde se almacenan los ficheros adjuntos, estando por defecto la ruta c:\temp que almacena el informe en el directorio raíz del OAS. Al haber en un mismo OAS más de un despliegue de VITROPATH y al utilizar la aplicación una secuencia numérica para identificar los ficheros subidos, se han solapado documentos con el mismo identificador.

  - Esta incidencia ha provocado que se hayan solapado ficheros adjuntos y se haya desindexado la documentación de pacientes que había sido adjuntada a la historia del paciente en VITROPATH. Otra consecuencia de este solapamiento es que se estaban visualizando informes asociados a un paciente por Servicios diferentes.

  Estos documentos adjuntos corresponden a peticiones e informes de pruebas realizadas en centros externos que se adjuntan al informe de VITROPATH.

- Se han analizado cada uno de los OAS donde está desplegado VITROPATH para determinar si otros Hospitales del SESCAM pueden haberse visto afectados, verificándose que la incidencia ha afectado a cuatro Hospitales adscritos al SESCAM.

Respecto a las medidas implementadas con anterioridad a la brecha de seguridad.

- Han elaborado un **Registro de Actividades de Tratamiento** (RAT), aportado a esta Inspección de Datos, con la descripción de las actividades involucradas en la brecha:

  "Historia Clínica del SESCAM" con la finalidad de Gestión de las Historias Clínicas de los Pacientes del SESCAM

  "Pacientes del SESCAM" con la finalidad de Control y gestión de los datos identificativos de los pacientes del SESCAM.

- No disponen de Análisis de Riesgos (AR) ni de Evaluaciones de Impacto de Protección de Datos (EIPD).

- Para el desarrollo del software existen controles consistentes en la realización de un plan de pruebas que se acuerda con la empresa contratada al efecto.

- Existe un procedimiento establecido en el Área de Tecnologías de la Información (ATI) del SESCAM para dar respuesta, a través de Grupos de Respuesta ante Incidentes Severos (GRIS), a incidencias ocurridas en los servicios de Tecnologías de la Información.

  Los Grupos de Respuesta a Incidentes Severos (GRIS) están compuestos por, al menos, una persona de cada una de las unidades funcionales del Departamento de Operación y Servicio del ATI y una persona del área funcional del Departamento de Proyectos del ATI relacionado con el Sistema de Información afectado.

  Entre las funciones y objetivos de dicho equipo de trabajo se encuentran la de recudir al máximo la incertidumbre en la organización de la situación ante incidentes severos, tomar decisiones adecuadas durante estos procesos, coordinar la actuación de los técnicos y hacer de enlace con la Dirección del ATI para mantenerles informados de la evolución del suceso. Coordinará las actuaciones necesarias para una recuperación rápida y eficiente de los Sistemas de Información afectados, de manera que la organización pueda operar con normalidad en el menor tiempo posible. Elaborará un informe en el que se detallará la evolución del incidente desde su detección y hasta la resolución este, indicando las medidas que deberían llevarse a cabo para evitar incidencias similares en lo sucesivo.

Respecto a las acciones y medidas tomadas ante la posible ocurrencia de la brecha.

- Notifican la brecha de seguridad a esta Agencia.

- Con ocasión de la brecha de seguridad ocurrida, aportan copia del informe elaborado por el GRIS, en el que se detalla e informa de la evolución del incidente,

desde su detección hasta la resolución de este y las medidas que la Organización ha adoptado para prevenir y evitar eventos similares en el futuro.

- Como medida concreta para evitar que se vuelva a producir un incidente igual en el informe del GRIS se indica que *"se han incluido en las pruebas en Producción del despliegue tareas específicas de inclusión de ficheros adjuntos y revisión de ubicación del archivo"*.

TERCERO: Con fecha 24/06/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al SESCAM, con NIF Q4500146H, por la presunta infracción de los artículos 5.1.f) del RGPD, conforme lo dispuesto en el artículo 83.5 del RGPD y 72.1.i) de la LOPDGDD, considerada muy grave a efectos de prescripción; y de los artículos 32 y 35.3.b) del citado RGPD, conforme lo dispuesto en el artículo 83.4 del RGPD y artículo 73, apartados d), e), f), g) y t) de la LOPDGDD, considerada grave a efectos de prescripción.

CUARTO: Con fecha 29/06/2020 se notificó el acuerdo de inicio al SESCAM, que no presentó alegaciones.

HECHOS PROBADOS

PRIMERO: El 09/09/2019 se detecta una incidencia indicando que desde el Hospital de Puertollano se estaban consultando documentos adjuntos en VITROPATH y aparecían documentos de otro Hospital.

Esta incidencia se comunicó directamente al proveedor de VITROPATH por correo electrónico en vez de comunicarla por el sistema de registro de incidencias IRIS tal como está protocolizado.

SEGUNDO: La incidencia tiene su origen en que en los despliegues de VITROPATH no se había configurado la ruta donde se almacenan los ficheros adjuntos, estando por defecto la ruta <<c:\temp>> que almacena el informe en el directorio raíz del OAS. Al haber en un mismo OAS más de un despliegue de VITROPATH y al utilizar la aplicación una secuencia numérica para identificar los ficheros subidos, se han solapado documentos con el mismo identificador.

TERCERO: Esta incidencia ha provocado que se hayan solapado ficheros adjuntos y se haya desindexada la documentación de pacientes que había sido adjuntada a la historia del paciente en VITROPATH. Otra consecuencia de este solapamiento es el acceso a informes asociados a un paciente por Servicios diferentes.

CUARTO: Se verifica que la incidencia ha afectado a cuatro Hospitales adscritos al SESCAM.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58, 64.2 Y 68.1 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

El RGPD define en el artículo 4:

1) «*datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*;"

2) «*tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*;

6) *«fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;*

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

De acuerdo con las definiciones transcritas e investigaciones realizadas se debe concluir que el responsable del tratamiento de los datos objeto de la citada brecha de seguridad es el SESCAM.

Los hechos notificados a esta Agencia por el SESCAM, en calidad de responsable del tratamiento, son constitutivos de infracción, imputable al SESCAM, por vulneración del artículo 5.1.f) del RGPD que indica:

<<1. Los datos personales serán:

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)>>.

Obligación que se modaliza en el artículo 5 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), que precisa:

<<1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.>>

El artículo 24 del RGPD, responsabilidad del responsable del tratamiento, dispone:

<< 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos>>.

El art 25 del RGPD establece las obligaciones que a continuación se indican:

<<1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.>>

El artículo 28.1 y 2 de la LOPDGDD, relativo a las obligaciones generales del responsable y encargado del tratamiento, señala lo siguiente:

<<1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.>>

El artículo 35.1 y 35.3.b) del RGPD, sobre la evaluación de impacto relativa a la protección de datos, señalan lo siguiente:

<<1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares>>.

<<3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10>>.

Conforme lo dispuesto en el art 35.4 del RGPD, la AEPD ha establecido y publicado una lista de los tipos de operaciones de tratamiento que requieren una evaluación de

impacto.

Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 *"Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD"*, los complementa y debe entenderse como una lista no exhaustiva:

(…)

<<4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos>>.

En el citado documento (WP248, página 15, III.c) señala lo siguiente:

<<El requisito de realizar una EIPD se aplica a operaciones de tratamiento existentes que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.

No será necesaria una EIPD para operaciones de tratamiento que hayan sido comprobadas por una autoridad de control o el delegado de protección de datos, de conformidad con el artículo 20 de la Directiva 95/46/CE, y que se realicen de una forma que no haya cambiado desde la anterior comprobación. De hecho, «[l]as decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas» (considerando 171).

En cambio, esto significa que deberán someterse a una EIPD los tratamientos cuyas condiciones de aplicación (alcance, fin, datos personales recogidos, identidad de los responsables o destinatarios del tratamiento, periodo de conservación de datos, medidas técnicas u organizativas, etc.) hayan cambiado desde la anterior comprobación realizada por la autoridad de control o el delegado de protección de datos y que probablemente entrañen un alto riesgo.

Además, podría requerirse una EIPD después de que se produzca un cambio de los riesgos a causa de las operaciones de tratamiento, por ejemplo debido a la puesta en marcha de una nueva tecnología o a que los datos personales se usan para un fin distinto. Las operaciones de tratamiento de datos pueden evolucionar rápidamente y pueden surgir nuevas vulnerabilidades. Por tanto, cabe señalar que la revisión de una EIPD no resulta útil solo para la mejora continua, sino que también es fundamental para mantener el nivel de protección de datos en un entorno que evoluciona con el tiempo. Una EIPD también puede resultar necesaria debido a cambios en el contexto organizativo o social de la actividad de tratamiento, por ejemplo debido a que los efectos de determinadas decisiones automatizadas hayan ganado importancia o a que nuevas categorías de interesados se vuelvan vulnerables a la discriminación. Cada uno de estos ejemplos podría ser un elemento que originase un cambio del riesgo resultante de la actividad de tratamiento en cuestión.

En términos de contexto, los datos recogidos, fines, funcionalidades, datos personales tratados, destinatarios, combinaciones de datos, riesgos (medios de apoyo, causas de riesgo, efectos posibles, amenazas, etc.), medidas de seguridad y transferencias internacionales.

En cambio, ciertos cambios también podrían reducir el riesgo. Por ejemplo, una operación de tratamiento podría evolucionar de forma que las decisiones ya no fueran automatizadas o una actividad de observación ya no fuera sistemática. En ese caso, la revisión del análisis de riesgo realizada puede mostrar que ya no se requiere la realización de una EIPD.

Por razón de buenas prácticas, una EIPD debe ser continuamente revisada y reevaluada con regularidad. Por tanto, incluso si el 25 de mayo de 2018 no se requiere una EIPD, será necesario, en el momento oportuno, que el responsable del tratamiento lleve a cabo una evaluación de este tipo como parte de sus obligaciones generales de responsabilidad proactiva.>>.
En consecuencia, deberá realizarse una EIPD si no se dispusiera de ella o, en su caso, revisar la existente y reevaluarla tras las nuevas modificaciones de los tratamientos de datos realizados en el ámbito del aplicativo VITROPATH.

III

El artículo 83.5 a) del RGPD, considera que la infracción de <<*los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9" es sancionable, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento, con multas administrativas de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*.>>

El artículo 83.4 a) del RGPD, indica: <<*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10. 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*: a) *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43>>*.

IV

El artículo 83.7 del RGPD indica:

<<*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro>>*

El artículo 58.2. b) y d) del RGPD indica lo siguiente:

<<*Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado>>.

Por su parte, el ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6 de la LOPDDGG:

<<1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.>>

V

En el presente caso, de las investigaciones llevadas a cabo por esta Agencia, se desprende que el SESCAM ha infringido el principio de confidencialidad al posibilitar indebidamente el acceso a los datos de salud de 431 pacientes por personal no autorizado. Igualmente, ha vulnerado el principio de integridad al no garantizar la seguridad de los datos de salud de 431 pacientes contra la pérdida, destrucción o daño accidental mediante la aplicación de medidas técnicas u organizativas apropiadas. Tampoco consta que el SESCAM haya realizado el adecuado análisis de riesgo y la preceptiva evaluación de impacto de conformidad con lo dispuesto en el art 35 del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a SERVICIO DE SALUD DE CASTILLA LA MANCHA, con NIF Q4500146H, por la infracción del artículo 5.1.f) del RGPD, conforme lo dispuesto en el artículo 83.5 del RGPD y 72.1.i) de la LOPDGDD, considerada muy grave a efectos de prescripción, una sanción de apercibimiento; y de los artículos 32 y 35.3.b) del citado RGPD, conforme lo dispuesto en el artículo 83.4 del RGPD y artículo 73, apartados d), e), f) y g) de la LOPDGDD, considerada grave a efectos de prescripción, una sanción de apercibimiento.

SEGUNDO: REQUERIR al SERVICIO DE SALUD DE CASTILLA LA MANCHA que aporte en el plazo de seis meses:

- Análisis de riesgos y evaluación de impacto de las operaciones de tratamiento de datos personales en el ámbito del aplicativo VITROPATH conforme lo dispuesto en el art 35 del RGPD.

- Auditoría tras la brecha de seguridad notificada que certifique que las operaciones de tratamiento de datos personales en el ámbito del aplicativo VITROPATH son conformes a lo dispuesto en el RGPD.

TERCERO: NOTIFICAR la presente resolución a SERVICIO DE SALUD DE CASTILLA LA MANCHA, con NIF Q4500146H y con domicilio en la Avenida Río Guadiana 4, 45071 Toledo.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

QUINTO: COMUNICAR la presente resolución a la CONSEJERIA DE SANIDAD DE CASTILLA LA MANCHA, con NIF S1911001D, Plaza Conde 2, 45002, Toledo.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa

si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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