- **Expediente N.º: EXP202413653**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes,

HECHOS

PRIMERO: En fecha 25/09/2024 se presentó reclamación ante la Agencia Española de Protección de Datos por hechos que podrían suponer una vulneración de la normativa de protección de datos imputables al SERVICIO EXTREMEÑO DE SALUD, con NIF Q0600413I (en adelante SES) en relación con un supuesto acceso indebido el 06/05/2024 por una empleada del Centro Médico ******LOCALIDAD.1*** a la historia clínica de la parte reclamante***.***

La parte reclamante señala que ***(…)*** y que el acceso se habría perpetrado ***(…).***

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación al SES, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 8/10/2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 7/11/2024 se recibe en esta Agencia escrito de respuesta indicando que:

*"No se ha tenido conocimiento de esta situación ni se ha recibido por parte de la reclamante comunicación o denuncia previamente.*
*Se inicia de oficio un expediente interno a efectos de conocer los hechos denunciados. Habiendo obtenido información sobre los accesos a la Historia Clínica de la denunciante en las fechas indicadas, se da traslado al área del Servicio Extremeño de Salud con capacidad y funciones suficientes para abordar esta denuncia para que realice las investigaciones oportunas e incoe, si procede, expediente administrativo."*

Sobre las causas que han motivado la incidencia que ha originado la reclamación y las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia, manifiesta que:

*"El sistema de información* ******SISTEMA.1*** *que sostiene la historia clínica única y electrónica en el Sistema Sanitario Público de Extremadura tiene implementado un sistema de control de acceso lógico por el que, en función del perfil de usuario que se*

*valide en el sistema, se accede a una u otra información y se tiene acceso a unas u otras aplicaciones.*
*Cuando un profesional sanitario accede a la historia clínica de un ciudadano se entiende que está legitimado cuando forma parte de su cupo, hay tratamientos activos o está citado en la agenda. Si no se dan esas circunstancias, es el profesional quien debe justificar el motivo del acceso.*
*Pese a la reciente sentencia de enero de 2024 de la AN que ratificaba el criterio de la AEPD, en cuanto que el ciudadano no tiene un derecho implícito a conocer quien, dentro de un sistema sanitario, accede a su historia clínica, en Extremadura, la Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente (desarrollo autonómico de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica) establece una obligación implícita para el SES al reconocerse, en el artículo 35.3 de dicha norma, el derecho del paciente "a obtener copias o certificados de los mencionados documentos, y a conocer en todo caso quién ha accedido a sus datos sanitarios, el motivo del acceso y el uso que se ha hecho de ellos". Así los ciudadanos de la comunidad autónoma de Extremadura pueden conocer esta información solicitándola a los servicios de documentación clínica de su área de salud e, incluso, a través de la aplicación Centro de Salud Online.*
*Este sistema de control de acceso lógico ya viene avalado por la propia AEPD que, en su resolución de archivo de actuaciones E/04418/2016:*
"*Ha quedado acreditado que el Servicio Extremeño de Salud dispone de un control de accesos que cumple con lo exigido por el RLOPD por cuanto el mencionado Servicio aportó documentación que acredita tal extremo siendo identificados el usuario, fecha y hora, tipo de acceso, que accedió a la historia clínica del denunciante, identificación posible gracias a la existencia de tarjeta identificativa del profesional, y su identificación como usuario del sistema con contraseña personal. El sistema recogió los accesos del médico denunciado con habilitación de "Gestión del paciente" y "Asistencial".*

*Cabe concluir por tanto que en el presente caso el sistema de información utilizado por el Servicio Extremeño de Salud, y que gestiona la historia clínica electrónica cumple con las medidas de seguridad exigidas por el art. 93 (control de accesos) y 103 (registro de accesos) del RLOPD, tendentes a evitar accesos no autorizados (art. 9 de la LOPD) al*
*acreditarse que se dispone de un control y un registro de accesos a las historias clínicas, así como de listas cerradas de usuarios con acceso a las historias clínicas dado su vinculación asistencial con los titulares de las mismas, y caso de no existir dicho vínculo, la existencia de medida de seguridad que impide el acceso a aquellos usuarios que no tengan dicho vínculo o una actividad programada con el paciente, exigiendo al usuario del sistema que en estos casos, incluya una justificación para el acceso a la historia clínica, justificación de la cual el sistema guarda registro de tal manera que puede comprobarse posteriormente la idoneidad o no de la referida justificación aducida por el profesional para efectuar el acceso a la historia clínica.*"

TERCERO: Con fecha 25/12/2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en

cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Se solicita información al SES y se obtiene respuesta el 25/4/2024 en la que se pone de manifiesto que:

- *"Consta un acceso a los datos de 06/05/2024 al historial médico de la parte reclamante por parte de* ***A.A.A.****. A continuación, la información extraída de la consulta a los logs de acceso del sistema:*

| ***Fecha*** | ***Hora*** | ***Motivo de acceso*** | ***Nombre de Usuario*** |
|---|---|---|---|
| 06/05/2024 | 9:14:46 | Asistencial | ***A.A.A.*** |

- *Los usuarios del sistema de información se corresponden con un único profesional. Cada usuario tiene además fijado un perfil, en función del cual tiene acceso o no a determinados aplicativos y, dentro de estos, se limitarán las funcionalidades a las necesarias para el desempeño del trabajo."*

  - Sobre las <u>medidas de control de acceso implantadas al historial médico</u>:
  "*La autenticación es personalísima, los usuarios son conscientes de que no deben compartir los usuarios y las contraseñas tal como se les recuerda en un aviso al inicio de la sesión. Los accesos están limitados en función del perfil del usuario y, además, sólo puede darse acceso a historiales para los que exista una legitimación a través de una relación previa (cupo, zona, agenda, tratamiento activo). De esta manera si un usuario del sistema va a acceder a un historial de un paciente debe contar con esa legitimación o, de no hacerlo, declarar -bajo su responsabilidad- el motivo del acceso. Los ciudadanos pueden consultar los accesos a la HC en cumplimiento de lo establecido en la Ley 3/2005 de Extremadura que desarrolla la Ley básica 41/2002."*

- Sobre el <u>resultado de la investigación interna sobre el acceso indebido al expediente de la reclamante y medidas implantadas</u>, en su caso, para evitar los accesos indebidos:
  *"Con fecha 04/11/2024 se envió información relativa a esta reclamación a la Subdirección de Personal del SES para que investigase y abriese, si procediera, el pertinente expediente. Se hizo así por ser esta subdirección la competente en esta materia. A efectos de poder dar respuesta a su solicitud se le ha preguntado por el estado de la investigación de la que se le informará cuando se reciba la información.*

Aporta documento con los accesos al historial médico de la parte reclamante donde consta el acceso reclamado.

Por otra parte, se comprueba en el Registro de Actividades de Tratamiento del Servicio Extremeño de Salud que la entidad responsable del tratamiento de Historias Clínicas (págs. 10-12) es la CONSEJERÍA DE SALUD Y SERVICIOS SOCIALES (en adelante, CCSS).

Se solicita información a la CSSS recibiéndose respuesta el 6/3/2026 en los siguientes términos:

1. Acreditar las medidas y mecanismos implementados tanto para identificar como autenticar a los usuarios del sistema de acceso a la historia clínica.

*"El sistema de información *****SISTEMA.1** cuenta con un sistema de control de acceso basado en usuario y contraseña, que permite a los usuarios acceder a la información de los pacientes estableciendo controles de acceso basados en el perfil de usuario. En *****SISTEMA.1**, hay tantos perfiles de usuario como perfiles profesionales y esto no se limita a perfiles genéricos sino que distingue a los profesionales por el lugar donde desempeña su trabajo. Así, no es lo mismo un perfil de un mismo profesional de atención primaria que de atención especializada o, no tienen las mismas características un usuario con un perfil administrativo dentro de un hospital en función del área en el que desempeña sus funciones. En resumen, cuando un profesional inicia sesión en el sistema de información del Servicio Extremeño de Salud, accede a una serie de aplicaciones en función del perfil del usuario; esto es, no solo medicina, enfermería, auxiliares, administración, celadores… sino que dentro de cada uno de estos perfiles, existen especialidades puesto no es lo mismo un administrativo de un centro de salud o de la gerencia, que uno que desempeñe su trabajo en un centro hospitalario e, incluso, dentro de estos, no todas las especialidades son iguales."*

2. Según la información proporcionada, el usuario accede a los datos del paciente por *"motivo asistencial"*, se solicita que confirmen si el usuario citado en su respuesta contaba con legitimación para el acceso (por relación previa de cupo, agenda o tratamiento activo) o por el contrario se accedió por un motivo distinto bajo la responsabilidad del propio usuario, y en tal caso, aportar la justificación que el sistema registró para este acceso.

*"El acceso al sistema de información del Servicio Extremeño de Salud es muy distinto en función de los distintos perfiles. En el caso de la atención sanitaria, el acceso a la historia clínica sólo se produce por personal sanitario que, una vez obtienen ese acceso, pueden acceder a la historia clínica completa, tal como ocurría en el formato papel y, con la legitimación del uso asistencia que cumple la finalidad de proteger intereses vitales del interesado.*
*El acceso a la información clínica sólo puede producirse sobre la base de la necesaria existencia de una relación que legitime el acceso del profesional sanitario a una determinada Historia Clínica. Por este motivo, al acceder al Historial de un paciente que se está tratando en ese momento en el puesto de trabajo clínico (sea Hospitalización, Consultas Externas, Pruebas Funcionales, Hospital de Día, Quirófano…), el sistema informático entiende de forma automática que el motivo de acceso es Asistencial, y así se refleja en dicho sistema. No obstante, este no es un proceso automático, sino que el sistema sólo permite el acceso a historiales de pacientes que, bien están bajo un tratamiento activo, bien están citados en la agenda del profesional o, bien pertenecen a los pacientes que tiene asignados en su cupo.*

*Cuando se accede al Historial médico mediante la búsqueda de un paciente (no seleccionándolo directamente de un listado de trabajo), el sistema obliga a elegir un motivo de acceso de entre los que están configurados para cada perfil. Entre ellos, en función del perfil de usuario pueden aparecer los siguientes:*

- *Gestión de Paciente: se selecciona cuando el acceso al Historial se relaciona con una acción que se va a realizar sobre un paciente que no se encuentra en el Puesto de Trabajo Clínico en ese momento, tal como consulta o revisión de documentación, realización de informes, preparación previa de consulta o intervención quirúrgica, revisión de órdenes clínicas y citaciones…*
- *Estudio de Investigación: se selecciona, como su propio nombre indica, cuando el acceso al Historial médico se relaciona con trabajos de investigación en los que está incluido ese paciente.*
- *Solicitud DCL: se usará cuando el acceso al Historial se realice para dar respuesta a una Solicitud de Documentación Clínica procedente del propio paciente o de alguna persona autorizada.*

*No obstante, aunque se haya establecido este filtro de acceso, ello no implica que el acceso sea total, puesto que cada uno de los motivos que legitimaría el acceso y que acaban de exponerse no implica el acceso sin restricciones a la información clínica. Por ello, cada uno de los accesos va acompañado de restricciones de acceso, puesto que no tendría sentido un acceso total a información sanitaria cuando el motivo que justifica el acceso es un motivo administrativo y no sanitario.*

*Previo a esto, en cada inicio de sesión se recuerda a los profesionales las obligaciones de confidencialidad y el necesario cumplimiento de las normativas internas respecto del acceso a la información. Todo ello completando las normativas que conocen los profesionales y que tienen disponibles en el Portal del SES (que es la puerta de acceso informática de todos los perfiles profesionales del SES) y sumado a otras medidas, tales como salvapantallas informativos, píldoras formativas, portal de conocimiento… en los que se recuerdan estas obligaciones.*

El 27/04/2024 se recibe contestación del SES al requerimiento efectuado el 06/05/2025 en el que se señala entre otros aspectos, lo siguiente:

*“Se dio traslado al área del Servicio Extremeño de Salud con capacidad y funciones suficientes para abordar esta denuncia para que realice las investigaciones oportunas e incoe, si procede, expediente administrativo. (…)*

*Respecto de la seguridad de la información en el SES, el sistema de información ***SISTEMA.1 que sostiene la historia clínica única y electrónica en el Sistema Sanitario Público de Extremadura tiene implementado un sistema de control de acceso lógico por el que, en función del perfil de usuario que se valide en el sistema, se accede a una u otra información y se tiene acceso a unas u otras aplicaciones.*

*Cuando un profesional sanitario accede a la historia clínica de un ciudadano se entiende que está legitimado cuando forma parte de su cupo, hay tratamientos activos o está citado en la agenda. Si no se dan esas circunstancias, es el profesional quien debe justificar el motivo del acceso”.*

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II

Tratamiento de datos de categoría especial

El artículo 9. del RGPD en relación con el tratamiento de categorías especiales de datos personales, establece:

"1. *Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico, racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física."*

*2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*
*a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*
*b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;*
*c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;*

*d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;*
*e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;*
*f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;*
*g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;*
*h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;*
*i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional*
*j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado."*

III

Seguridad del tratamiento

El artículo 32 del RGPD estipulan lo siguiente:

*"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
*a) la seudonimización y el cifrado de datos personales;*
*b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*

*c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
*d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

*2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.*

*3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.*

*4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."*

## IV
## Conclusión

Debe señalarse que el responsable del tratamiento es la persona física o jurídica, pública o privada que decide sobre fines y medios en relación con el tratamiento de datos personales. Así, el responsable del tratamiento en el sentido del RGPD, cuando se trata de una persona jurídica es la propia organización, y no una persona o unidad dentro de la misma, aunque cuando esta última sea, en la práctica, quien lleve a cabo el tratamiento material de datos para el cumplimiento de los fines y con los medios determinados por el responsable del tratamiento.

El hecho de que una persona, unidad o departamento de una organización se le haya asignado entre sus funciones la realización de un tratamiento de datos, no implica que esta persona, unidad o departamento devenga responsable del tratamiento en lugar de la organización en su conjunto.

Al contrario, el responsable del tratamiento responde por sus empleados, así como por sus encargados del tratamiento, tal y como señala el artículo 29 del RGPD, pues estos actúan bajo su autoridad y siguiendo sus instrucciones. Esto ocurre en el ámbito sanitario respecto al tratamiento de datos personales realizado por los facultativos y otro personal sanitario, quienes tienen acceso a la historia clínica de sus pacientes conforme al artículo 16.5 de la LAP.

No obstante, cuando un facultativo accede a historias clínicas de personas con los que no le une relación asistencial alguna, ni relación médico-paciente, y contraviene las instrucciones del hospital o centro sanitario, pasa a realizar un tratamiento de datos personales para sus propios fines, extralimitándose de manera ilícita en el ejercicio de las funciones que tiene atribuidas, deviniendo, por tanto, responsable del tratamiento.

En estos términos se pronuncian las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD:

*"19. En principio, todo tratamiento de datos personales realizado por empleados en el ámbito de las actividades de una organización se presumirá realizado bajo el control de dicha organización. No obstante, es posible que, en casos excepcionales, un empleado decida usar datos personales para sus propios fines, extralimitándose de manera ilícita en el ejercicio de las funciones que se le hubieran atribuido (p. ej., con vistas a crear su propia empresa o algún fin similar) (…).* (El subrayado es de la AEPD).

En esos casos, asegura el CEPD *"recae en la organización, en calidad de responsable del tratamiento, el deber de asegurar que se hayan aplicado medidas técnicas y organizativas apropiadas, incluyendo, p. ej., la prestación de formación e información a los empleados con vistas a garantizar el cumplimiento del RGPD*".

En el presente caso, se presentó una reclamación ante la AEPD por un supuesto acceso indebido a la historia clínica de la parte reclamante (quien presta sus servicios en un centro médico del SES), por una facultativa compañera de trabajo, sin su consentimiento.

Debe precisarse, no obstante, que el acceso a la historia clínica por parte de un facultativo en el ejercicio de sus funciones, no se ampara en el consentimiento del interesado.

Por otra parte, durante las actuaciones previas de investigación realizadas, si bien se ha confirmado el acceso a la historia clínica de la parte reclamante, en la fecha señalada por esta, no ha podido acreditarse que dicho acceso fuera indebido. Así, no ha podido comprobarse que el acceso no se realizara en el ejercicio de las funciones del facultativo en cuestión.

En otro orden de cosas, se ha constatado que el SES contaba con diferentes medidas y protocolos sobre el acceso y uso de historias clínicas. Así, entre otros, los accesos de los usuarios a la aplicación de la historia clínica están limitados en función del perfil del usuario y sólo se da acceso a historiales para los que exista una legitimación a través de una relación previa (cupo, zona, agenda, tratamiento activo).

A este respecto, debe destacarse que en el ámbito administrativo sancionador son de aplicación, con alguna matización, pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones.

El Tribunal Constitucional en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta:

> "*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas*

> *practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio*".

De acuerdo con este planteamiento, el artículo 53.2 de la LPACAP, establece que, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

> *"b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

Como ha precisado el Tribunal Supremo en Sentencia de 26 de octubre de 1998, la vigencia del principio de presunción de inocencia

> *"no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo."*

Así las cosas, se debe distinguir la verdadera prueba de indicios de las meras sospechas o conjeturas. El Tribunal Constitucional ha manifestado en su Sentencia 24/1997 que

> *"los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que: a) La prueba indiciaria ha de partir de hechos plenamente probados. b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)."*

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado indicios racionales suficientes que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al SERVICIO EXTREMEÑO DE SALUD (SES) y a la parte reclamante.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia 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.

940-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos