- Expediente N.º: EXP202310460

RESOLUCIÓN DE ARCHIVO DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: Con fecha 13 de julio de 2023 se interpuso reclamación ante la Agencia Española de Protección de Datos (en adelante, AEPD) por una posible infracción imputable a ***A.A.A.*** con NIF******NIF.1*** (en adelante, ***A.A.A.*** o parte reclamada).

Los hechos que se ponen en conocimiento de esta autoridad son:

El ******PUESTO.1*** del ******CENTRO.1,*** reclama contra siete compañeras facultativas del mismo servicio (entre las que se encuentra ***A.A.A.***), por sospechar accesos indebidos a su historia clínica. Afirma que una de ellas encargó a una agencia de detectives el seguimiento de su persona, siendo que en el informe que emitió esta agencia, aparece como su dirección la que figura, exclusivamente, en su historia clínica en el referido hospital. Dicho informe habría sido utilizado por las reclamadas, para presentar una denuncia contra el reclamante, ante ***DEPARTAMENTO.6 del señalado hospital.
Asimismo, manifiesta que ha presentado denuncia por estos hechos ante ***DEPARTAMENTO.6 del ******CENTRO.1 (***en adelante ******CENTRO.1)***, quien habría elevado el asunto al organismo encargado de protección de datos de la ******CCAA.1***.

Junto a su escrito aporta:

- Documento de una página y sin firma, con título INFORME 78-22, por el que se encomienda a la ******EMPRESA.1***, realizar investigaciones sobre el reclamante en la dirección postal ******DIRECCIÓN.1***. (Anexo I)
- Parte superior de pantalla PC donde aparece el número de historia clínica del reclamado, su nombre y la dirección postal ******DIRECCIÓN.1*** (Anexo II).
- Solicitud de apertura de proceso por acoso laboral dirigida a ***DEPARTAMENTO.1 del ******CENTRO.1*** con de fecha registro de entrada en ***DEPARTAMENTO.2 de la ******CCAA.1*** el 07/07/2023 (Anexo III).
- Solicitud de *auditoría a* ***A.A.A.*** *por accesos ilegítimos* a historias clínicas, dirigida a ***DEPARTAMENTO.1 del ******CENTRO.1*** con de fecha registro de entrada el 05/06/2023 (Anexo IV).
- Documento nombrado como Anexo V que es idéntico al Anexo IV.

En fecha 14 de julio de 2023 la parte reclamante amplió el contenido de la reclamación, en este caso exclusivamente contra ***A.A.A.*** "*por accesos indebidos a historias clínicas, utilizar las redes sociales (*******APP.1*** *y* ******APP.2****) para enviar datos de salud de pacientes, en algunos casos con los que no tiene función asistencial y quejarse de la carga asistencial, además de no guardar las medidas mínimas de seguridad, dejando su ordenador abierto y marchándose, exponiendo a la vista de todos los datos que contiene".*

Aporta capturas de pantalla de la aplicación de mensajería instantánea ******APP.1*** o similar y fotografías tomadas, del supuesto puesto de trabajo de la reclamada, con el PC abierto con datos expuestos. Por otro lado, alega que ha solicitado al hospital una auditoría sobre accesos indebidos a historias clínicas de diferentes pacientes, realizados por la facultativa reclamada.

La documentación que aporta la parte reclamante es:

- Anexo I: 19 capturas de pantalla de conversaciones en aplicaciones de mensajería instantánea, como ******APP.1*** o similar y 3 fotografías de lo que parecerían aplicaciones informáticas en un PC.
- Anexo II: listado de puestos ocupados *por* ***A.A.A.***

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 Delegado de Protección de Datos del ******ORGANISMO.2***, 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 5/09/2023 tiene entrada en la AEPD contestación al mencionado traslado, mediante el aporte de la siguiente documentación:

- Anexo I.- Cláusula Informativa Pacientes. Dicha cláusula está presente en todas las plantillas de informes que se descargan desde ******SISTEMA.1***.
- Anexo II.- Informe de auditoría de accesos a la Historia Clínica (HC) de la parte reclamante.
- Anexo III.- Informe de auditoría de uso de sistemas de información y log de accesos correspondientes a 10 historias clínicas y sus fechas.
- Anexo IV.- Solicitud de auditoría de accesos a HC.
- Anexo V.- Solicitud de auditoría de sistemas de información.
- Anexo VI. - Respuesta al interesado.
- Anexos VII y VIII.- Propuesta de iniciación de procedimiento disciplinario.
- Anexo IX.- Solicitud de Información al CDPD.
- Anexo X.- Informe del CDPD.
- Anexo XI.- Informe de ***DEPARTAMENTO.3 ******CENTRO.1*** al CDPD.
- Anexo XII: Acuse de recibo
- Anexo XIII: Acuse de recibo.
- Anexos XIV y XV: Correos electrónicos al personal del ******CENTRO.1*** recordando la importancia de conocer la normativa vigente.

En el informe del CDPD de ***ORGANISMO.1 de la ******CCAA.1,*** entre otros aspectos, se pone de manifiesto:

"PRIMERA. - La historia clínica (HC) *es el "conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial", tal y como se define en el artículo 3 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, (en adelante, LAP).*

El fin principal de la historia clínica es "[…] facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud" (art.15.2 LAP).

Por su parte, el apartado 5 del artículo 16 LAP dispone: "El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria".

La base jurídica que legitima el tratamiento de HC la encontraríamos en el artículo 6.1 c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD): "el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento".

*Así pues, dicho tratamiento efectuado dentro de las competencias atribuidas a ***ORGANISMO.1* de la ******CCAA.1** encontraría habilitación legal en la propia Ley 14/1986, de 25 de abril, General de Sanidad; así como en la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la ***CCAA.1.*

Por otro lado, hay que tener en cuenta que estamos ante un tratamiento de datos de salud, categoría especial de datos de carácter personal, lo que implica que sólo pueden tratarse en determinadas circunstancias. No obstante, en el presente caso, el tratamiento quedaría habilitado de acuerdo con lo establecido en el artículo 9.2 h) del RGPD:

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.", todo ello basado en las referidas normas con rango de Ley.

*Por último, las categorías de interesados a indicar en ese escenario son los pacientes. La información que se les facilita relativa a protección de datos se puede observar adjunta en el Anexo I.- Dicha cláusula está presente en todas las plantillas de informes que se descargan desde *****SISTEMA.1** (aplicativo para gestionar la historia clínica de los pacientes).*

SEGUNDA. - […], queda totalmente acreditado que por parte del responsable -tal y como se desprende de la documentación adjunta- se da el debido cumplimiento al artículo 24 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), dónde se indica que:

"1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.(…)

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Así pues, se evidencia la efectividad de dichas medidas, toda vez que, a través del análisis de las trazas que se recogen en el sistema ******SISTEMA.1****, ha podido conocerse tanto el acceso efectuado como la actividad llevada a cabo por las facultativas en la HC del interesado; igualmente se han podido analizar los accesos a HC concretas solicitados, véase el Anexo II.- Informe de auditoría de accesos a HC y Anexo III.- Informe de auditoría de uso de sistemas de información.*

A su vez, es importante destacar que no se ha producido una vulnerabilidad de las medidas de seguridad del sistema de información, sino un incidente puntual y aislado producido por dos usuarias autorizadas que han efectuado un uso ilegítimo de la información vulnerando las políticas y normativa del responsable.

[…], cabe destacar que el Centro en todo momento ha actuado de forma proactiva y diligente a la hora de realizar las correspondientes investigaciones, así como dar contestación a las reclamaciones interpuestas por el interesado, tal y como puede observase en el Anexo IV.- Solicitud de auditoría de accesos a HC Anexo V.- Solicitud de auditoría de sistemas de información y Anexo VI.

Por tanto, queda reflejado que el Hospital cuenta con procedimientos y protocolos internos de actuación para que situaciones como las acontecidas no vuelvan a producirse, así pues, tras conocer los hechos, se pusieron inmediatamente en conocimiento del ******SERVICIO.1 (…)***, actuando con la diligencia debida a la hora de detectar y corregir cualquier abuso de las políticas y sistemas del centro, véase los Anexos VII y VIII.- Propuesta de iniciación de procedimiento administrativo.

*Cabe mencionar las obligaciones a las que están comprometidos los profesionales de ***ORGANISMO.1 conforme a la ORDEN 491/2013, de 27 de junio, de ***ORGANISMO.1, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de ***ORGANISMO.1 de la* ******CCAA.1,*** *dónde en su artículo 12 se indica:*

*"1. El personal que preste servicios en ***ORGANISMO.1 tiene la obligación de conocer y cumplir esta política y demás normativa de seguridad derivada de ella, siendo responsabilidad del Comité el que llegue a todos los usuarios.*

*2. Asimismo, se encuentran obligados todos los usuarios de los sistemas de información de ***ORGANISMO.1 a cumplir el "Decálogo de buenas prácticas para usuarios de sistemas de información de ***ORGANISMO.1"****,*** *que figura como anexo de este documento."* Ver Diligencia Orden Decálogo.

En este sentido el referido Decálogo establece, en el tratamiento y uso de datos de carácter personal, la siguiente obligación:

"3.1. Los usuarios deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la que esté autorizado".

10.1 Cuando los usuarios se ausenten del puesto de trabajo o dejen desatendido el ordenador deberán activar el sistema de bloqueo del que disponga su equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etcétera) con el fin de

que no se visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.

Asimismo, dicho decálogo recoge que "el incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente Decálogo de buenas prácticas podrá dar lugar a la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar, en aplicación de las normas reguladoras del régimen jurídico disciplinario propio del usuario".

Por todo ello, cabe hacer hincapié, tal y como ya hemos mencionado anteriormente, que por parte del Hospital se puso en marcha un protocolo interno de cara a implementar las acciones correctoras que fueran necesarias y depurar así las posibles responsabilidades.

TERCERA. - […] el tratamiento descrito de historia clínica es un tratamiento que se viene realizando con anterioridad a la aplicación del RGPD, esto es, bajo la vigencia de la derogada Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal. Por tanto, en base a que el tratamiento se inició bajo el marco normativo antiguo y según lo establecido por el propio RGPD, puesto que el alcance sigue siendo el mismo y no se ha producido ningún cambio tecnológico ni funcional al respecto, no cabría aplicar el punto 1 de artículo 35 RGPD y, por ende, no sería necesario la realización de una evaluación de impacto.

No obstante, si bien no se ha realizado una EIPD sobre este tratamiento en cuestión por lo anteriormente indicado, sí que debe subrayarse que se han realizado otras EIPD en cuanto a la gestión y tratamiento de las historias clínicas (HC) de los pacientes, en tanto en cuanto se han producido cambios en el alcance de ciertos tratamientos que tienen relación directa con la HC. En concreto, cabe hacer mención a dos evaluaciones de impacto que derivaron de las iniciativas de la Unión Europea para facilitar el desarrollo de sistemas de salud electrónica y su interoperabilidad entre Estados miembros.

Así pues, dichas EIPDs se efectuaron con motivo del cambio de alcance en la historia clínica, puesto que el mismo se ampliaba como consecuencia del intercambio de información clínica, del Sistema HCDSNS (Historia Clínica Digital del Sistema Nacional de Salud) y receta médica electrónica del Sistema RESNS (Receta Electrónica del Sistema Nacional de Salud) con la eHDSI (eHealth Digital Services Infrastructure), como parte del proyecto CEF (Connecting Europe Facility) para e-Salud de la Unión Europea.

*Es por esto que el 19/08/2021 y el 24/03/2022 se materializan desde ***ORGANISMO.1* de la ******CCAA.1*** *a través de ***DEPARTAMENTO.4* y ******DEPARTAMENTO.5***, *respectivamente como responsables del tratamiento, las dos evaluaciones de impacto relativas a los proyectos mencionados, analizando de este modo la operación de tratamiento tanto de intercambio de historia clínica como de dispensación electrónica de productos farmacológicos prescritos a ciudadanos pertenecientes de la UE, analizando las medidas de seguridad y la afectación de los derechos de los ciudadanos por ambos tratamientos en sus historias clínicas, ambas con un nivel de riesgo aceptable; firmadas por el Comité Delegado de Protección de Datos y posteriormente auditadas por el Ministerio de Sanidad, donde se logró verificar su cumplimiento y habiéndose superado las auditorías satisfactoriamente.*

CUARTA. - "La decisión adoptada a propósito de esta reclamación", señalar nuevamente que por parte del ******CENTRO.1***, *tras las reclamaciones interpuestas*

*primero ante ***DEPARTAMENTO.6 del Hospital y paralelamente ante la AEPD, se dio respuesta al interesado indicándole que, una vez analizada la situación sobre los hechos acaecidos, se había procedido a trasladar la misma a los organismos competentes, adoptando así las medidas oportunas al efecto.*

Tal y como se desprende de la documentación aportada, en fecha 05 y 12 de junio de 2023 respectivamente, B.B.B., presenta ante el ******CENTRO.1*** *escrito requiriendo auditoría e informe referente a: (I) accesos indebidos a HC de pacientes, así como al uso inadecuado de los sistemas de información del centro y equipamiento informático por parte de una de las facultativas y (II) los accesos que se han producido en su HC por parte de siete profesionales que trabajan en el Centro.*

*En cuanto a la primera solicitud presentada el día 05 de junio de 2023 la cual se puede observar en el Anexo 1 de la reclamación presentada por el interesado ante la AEPD, desde ***DEPARTAMENTO.3* del ******CENTRO.1*** *se solicita a* ***PUESTO.2 *que verifique -en relación con unas fechas e historias clínicas concretas - si se han realizado dichos accesos y cuando, así como una auditoria sobre su equipo de trabajo supuestamente asignado(I). En dicha solicitud, el interesado reclama que una de las facultativas estaría accediendo de forma habitual a historias clínicas para para las que, según indica, no tendría relación asistencial directa****.***

Tras conocer esta información el Centro procede a realizar la auditoría correspondiente y presenta un informe en el que se recoge que la profesional accedió a nueve de las diez HC comunicadas, remitimos a los Anexos III y V. No obstante, si bien el interesado manifiesta que no existiría relación asistencial para dichos accesos, desde el ******CENTRO.1*** *indican tal y como se desprende del Anexo XI que la facultativa es ***PUESTO.3, la cual se encarga del análisis de incidentes de seguridad y sucesos adversos que selecciona y analiza casos declarados en* ******ORGANISMO.1****, por lo que habría podido acceder en el ámbito de sus funciones y competencias.*

Respecto a la segunda solicitud presentada el 12 de junio de 2023, una vez el ******CENTRO.1*** *tiene constancia de ello, remite un Informe al Comité Delegado de Protección de Datos en fecha 26 de junio de 2023, adjunto como Anexo IX.- Solicitud de Información al Comité Delegado de Protección de Datos solicitando indicaciones y asesoramiento de cómo proceder en el último caso descrito (II). Asimismo, el propio Comité da respuesta a dicha solicitud a través de otro informe, adjunto como Anexo X.- Informe elaborado por el Comité Delegado de Protección de Datos, en el que se recoge que, ante las sospechas de posibles accesos no autorizados a historias clínicas, debe acudirse a la comprobación de las trazas y comunicar las averiguaciones a los órganos competentes que deban conocer el asunto en aras de depurar las posibles responsabilidades.*

*En base a esto, el 14 de agosto de 2023 desde ***DEPARTAMENTO.3* del ******CENTRO.1*** *solicitan a ***PUESTO.2 que realice las auditorías de accesos en* ******SISTEMA.1*** *en relación a la HC del interesado y referente a las profesionales referenciadas, véase Anexos IV y V.*

En relación a lo descrito, se elaboran los Informes que se adjuntan como Anexos II y III.

Por último, en fecha 18 de agosto de 2023, se da traslado y contestación a B.B.B. -Anexo VI- indicando que las auditorías solicitadas han sido oportunamente cursadas (previa consulta al CDPD), que se han detectado accesos total o parcialmente indebidos y que, por ello, dicha situación ha sido elevada desde el servicio de Asesoría

Jurídica del ***CENTRO.1 a los organismos competentes para que procedan en consecuencia*, Anexo VII y Anexo VIII.*

*QUINTA. - En lo relativo al punto 7 del requerimiento, en el que se solicita "Informe sobre las causas que han motivado la incidencia que ha originado la reclamación". Se pone de manifiesto que, desde el CDPD de ***ORGANISMO.1* de la ***CCAA.1,** y dentro de las funciones y competencias que tiene atribuidas, se solicitó a ***DEPARTAMENTO.6* del ***CENTRO.1**, que llevaran a cabo las investigaciones oportunas con el fin de determinar la concurrencia de los hechos señalados en la reclamación, así como que se informara sobre las actuaciones llevadas a cabo.*

*En este punto, remitimos tanto al Informe elaborado por parte de ***DEPARTAMENTO.3* del ***CENTRO.1,** Anexo XI.- Informe Dirección Gerencia, como a la contestación trasladada al interesado y acuse de recibo de la misma, véase también Anexo VI, XII y XIII.*

*SEXTA. - "Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia", señalar lo remitido por el ***CENTRO.1**, en el punto 3 del documento que se adjunta como Anexo XI.*

*Así pues, cabe destacar que, el responsable del tratamiento, con fin de dar cumplimiento al principio de responsabilidad proactiva contemplado en el artículo 5.2 del Reglamento General de Protección de Datos, ha adoptado una serie de medidas encaminadas a disminuir el riesgo de que situaciones como las acontecidas vuelvan a producirse. Por ello, el Centro, tanto el 14 de septiembre de 2022 como, nuevamente, el 16 de agosto de 2023, envía varios correos electrónicos al personal del Hospital recordando la importancia de conocer la normativa vigente aplicable, así como los documentos informativos que se pueden encontrar en la web del ***ORGANISMO.2* o de la ***CCAA.1**, recalcando que deben utilizarse medios institucionales en el desempeño de la actividad laboral, evitando el uso de recursos particulares como ***APP.1** o correos electrónicos personales.*".

*Asimismo, también se adjunta en dicho correo -a modo recordatorio- la Orden (…), por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de ***ORGANISMO.1 de la ***CCAA.1**. En la misma, como ya se ha mencionado anteriormente, se recoge el "Decálogo de buenas prácticas para usuarios de sistemas de información de ***ORGANISMO.1", de obligado cumplimiento para todo el personal que preste servicios en la Consejería.*

*Para finalizar y por todo lo anteriormente expuesto, queda evidenciado que el ***CENTRO.1** cuenta con una serie de medidas establecidas a fin de mantener y consolidar la seguridad de la información y privacidad, como por ejemplo la conservación de las trazas de acceso, la realización periódica de formaciones dirigidas al personal, así como el envío continuo de píldoras, recomendaciones y decálogos de buenas prácticas y que las actuaciones efectuadas por las profesionales sanitarias se han realizado saltándose los procedimientos y protocolos establecidos por el Centro así como por la Política de Seguridad de ***ORGANISMO.1.*

En lo referente a lo denunciado en la ampliación de la reclamación presentada el 14/07/2023, el ***ORGANISMO.2**, pone de manifiesto:

- Acceso por ***A.A.A.***, a historias clínicas para las que no parece tener autorización o legitimidad, por no tener relación asistencial con estos pacientes (Anexo III): ***DEPARTAMENTO.3 **del ****CENTRO.1*** confirma que ***A.A.A.*** accedió a 9 de las 10 historias de pacientes comunicados por la parte reclamante, sin embargo, debe considerarse que es ***PUESTO.3, comisión encargada del análisis de incidentes de seguridad y sucesos adversos que selecciona y analiza casos declarados ***(…).*** El ****CENTRO.1*** señala, además, que cualquier integrante de la ****ORGANISMO.3*** en el ejercicio de las competencias que le corresponden, podrá tener que acceder a toda o parte de la información correspondiente a cualquier proceso asistencial que sea requerida, para la investigación de cualquier incidente de seguridad comunicado a la ****ORGANISMO.3***. No quedando por tanto demostrado que el acceso a dichas historias clínicas no tuviera justificación en cuanto a su finalidad asistencial.
- Uso, por ***A.A.A.***, de redes sociales en su ámbito laboral: el ****CENTRO.1*** concluye en un uso inadecuado de redes sociales con desatención de las indicaciones de ***DEPARTAMENTO.6 y de la normativa de ***ORGANISMO.1 por parte de ***A.A.A.*** En consecuencia, ***DEPARTAMENTO.3 del ****CENTRO.1*** señala que, dado que los hechos manifestados por el reclamante, y verificados por el ****CENTRO.1***, podrían ser objeto de sanción disciplinaria, traslada el expediente al ****SERVICIO.1*** del ****ORGANISMO.2,*** quien a la vista de la petición cursada y en virtud de las competencias atribuidas, acuerda incoar (...) a ***A.A.A.***

En consecuencia, los posibles accesos generalizados a historias clínicas por la parte reclamada, así como el posible uso indebido de las redes sociales por esta, no son objeto del procedimiento sancionador.

TERCERO: Con fecha 12/09/2023 y de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación.

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 VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

Al objeto de investigar los hechos descritos, por esta Agencia el 16/01/2024 se realiza solicitud de información al ****ORGANISMO.2***, dando respuesta a la misma, el 6/02/2024, el Comité Delegado de Protección de Datos (CDPD) de ***ORGANISMO.1 de la ****CCAA.1 (***ORGANISMO.1).*** A la vista de la información proporcionada, se solicita ampliación de la información aportada, obteniéndose respuesta en fecha 3/10/2024.

A raíz de estas informaciones, se tiene conocimiento de lo siguiente:

1. ***SISTEMA.1***

***SISTEMA.1** es la aplicación de Historia Clínica Electrónica (HCE) que se utiliza en ***ORGANISMO.1 de la ***CCAA.1.**

La Historia Clínica (HC), conforme a la propia definición 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 (en adelante, LAP), constituye el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Su fin principal es facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Por tanto, es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente, aunque se pueden usar para otros fines (judiciales, epidemiológicos, de salud pública, de investigación o de docencia y comprobación de la calidad de la asistencia).

Para facilitar la continuidad de la asistencia en el año 2010 se aprobó el conjunto de datos que, por su importancia, deben estar contenidos en los informes clínicos más relevantes que describen los procesos de atención sanitaria realizados a ciudadanos concretos en cualquier centro o servicio del Sistema Nacional de Salud (Conjunto Mínimo de Datos de los Informes Clínicos CMDIC). La historia clínica electrónica es el registro en el que se archiva, en soporte electrónico, toda la información referente al paciente y a su atención. La información contenida en la historia clínica electrónica debe garantizar la calidad y seguridad en la atención al paciente.

La información y documentación clínica que gestiona se organiza en unidades básicas de información denominadas “objetos clínicos”, y a ella pueden acceder los distintos profesionales según su perfil y permisos de accesos.

El CDPD indica que, en el sistema de gestión de historias clínicas, existe una segregación de perfiles para la utilización de la herramienta, en base al desempeño de trabajo de cada uno de los puestos, y que se da cumplimiento al principio de mínimo privilegio, de conformidad con lo estipulado en el Esquema Nacional de Seguridad, limitando a cada usuario a lo mínimo estrictamente necesario para cumplir sus obligaciones:

> *“Los profesionales que acceden a *****SISTEMA.1** y a estos tipos de documentación e información son sanitarios de distintas Categorías y Perfiles Profesionales (facultativos y sanitarios no facultativos) de las distintas Unidades y Servicios, así como personal No Sanitario que participan en el proceso asistencial.*
>
> *Los perfiles y privilegios de acceso a *****SISTEMA.1** de cada uno de ellos se configuran según los roles, privilegios y permisos correspondientes, utilizando el módulo de Administración de *****SISTEMA.1** y las facilidades que proporciona. Por tanto, con carácter general el acceso a la Historia Clínica por parte de los profesionales sanitarios con fin asistencial está limitado a su rol.*
>
> *La configuración del área de Trabajo de las distintas Categorías y Perfiles, así como los elementos que componen esta área de trabajo (vistas, menú y opciones, permisos y privilegios) se realiza en razón al desempeño de la labor de cada profesional y grupo de profesionales al que pertenecen, según sus competencias y su participación en el proceso asistencial.*

Es por ello que dicha configuración se ha realizado teniendo en cuenta las restricciones necesarias para garantizar la prestación de una asistencia sanitaria adecuada a los pacientes. Esta dinámica pretende garantizar una asistencia segura y evitar posibles riesgos sanitarios por no estar disponible información clínica de interés en todo momento para los profesionales que pueden tener que asistir al paciente.

No obstante, esta flexibilidad de acceso a HCE por parte de los profesionales está regulada por la normativa vigente y siempre debe responder a una finalidad concreta que justifique el acceso y cuente con la debida autorización".

En el Anexo I se recoge también que, actualmente, ******SISTEMA.1*** permite restringir procesos concretos de una historia clínica, en determinados supuestos que describe, y permite habilitar la restricción de acceso a una historia clínica completa, en casos excepcionales, por los riesgos que conlleva y que también se describen.

- En cuanto a los sistemas de control de acceso se señala:
    - *Gestión de usuarios y claves de acceso: todos los usuarios con acceso a* ******SISTEMA.1*** *son usuarios de* ******SISTEMA.2*** *y como tal se gestionan en aplicativo* ******SISTEMA.3*** *y según la política corporativa establecida, y atendiendo al cumplimiento del Indicador de Control Usuarios ***SISTEMA.2 con acceso SSII del Contrato Programa y a la "Instrucción para el refuerzo de la seguridad sobre la identidad de los usuarios identificados en la red de Sanidad".*

      Se aporta como Anexo III el procedimiento establecido para la gestión de usuarios y claves de acceso a los sistemas de información, *Procedimiento gestión altas, bajas, modificación de usuarios del* ******CENTRO.1.***
    - *Estructura de perfiles de acceso: siguiendo en todo caso la política de mínimos privilegios.*
    - *Las políticas de acceso a sistemas de información son las institucionales:*
        - *ORDEN 491/2013, de 27 de junio, de ***ORGANISMO.1, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración Electrónica y de los sistemas de información de ***ORGANISMO.1 de la ***CCAA.1.* .
        - *"Instrucción para el refuerzo de la seguridad sobre la identidad de los usuarios identificados en la red de Sanidad"* ***(…)*** *Sep. 2023.* ***.***
            - *Recomendaciones de Estilo para los profesionales del* ******CENTRO.1*** *(Basado en Recomendaciones de Estilo para profesionales del* ******ORGANISMO.2****). Edición marzo 2019*. Anexo IV *[…]*
                - *4.1.1.-COMUNICACIÓN ESCRITA*

                  REDES SOCIALES

                  En ningún caso, los profesionales pueden utilizar las redes sociales como medio para atender a los pacientes

o facilitarles algún tipo de información clínica, debiendo recurrir para esto a los canales ordinarios.

*Cuando un profesional del *****ORGANISMO.2** tenga presencia en las redes sociales debe tener en cuenta que todas sus publicaciones serán a título personal y nunca como portavoz de su centro de trabajo o de la organización, asumiendo las responsabilidades legales y penales que pudieran derivarse de sus publicaciones.*

[…]

- *5.- CONFIDENCIALIDAD E INTIMIDAD*

  Sólo las personas autorizadas pueden acceder a las aplicaciones informáticas, utilizando su clave de acceso personal e intransferible. La aplicación debe quedar cerrada al finalizar.

  […]

  2. ¿Estás seguro de que tienes que acceder a esa historia clínica? Piénsalo. Sólo debes acceder si es necesario para los fines de tu trabajo.

  3. Recuerda: tus accesos a la documentación clínica quedan registrados en el sistema. Se sabe en qué momento y a qué información has accedido. Los accesos son auditados posteriormente.

  4. Evita informar a terceros sobre la salud de tus pacientes, salvo que éstos lo hayan consentido o tengas una justificación lícita.

  5. Cuando salgas del despacho asegúrate de cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente, contacta con el departamento de informática.

  6. No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si fuera imprescindible, no olvides cifrar los datos.

  […]

  9. No dejes las historias clínicas a la vista sin supervisión.

  10. No crees por tu propia cuenta, ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informática".

- <u>En cuanto a la asignación de permisos se indica:</u>

  *"Según el procedimiento de Gestión de Usuarios establecido, los usuarios autorizados con acceso a *****SISTEMA.1**, siempre usuarios que tengan usuario en ***SISTEMA.2 y éste esté activo en la unidad organizativa correspondiente, cuando se les da de alta en *****SISTEMA.1** se le asigna junto con otros Datos*

*Personales el Rol y la Categoría Profesional que les corresponden **(…)** en base a los cuales ya van a heredar unos permisos y privilegios embebidos en la propia lógica de la aplicación *****SISTEMA.1**, igualmente ocurre con el resto de los atributos que se le asocian en la ficha de alta usuario en *****SISTEMA.1** (Datos Asistenciales **(…)**, Seguridad **(…)**), Unidades de gestión (**…**) y Grupos. Respecto a la asignación de grupos, se les asigna por defecto un grupo general con los permisos y privilegios correspondientes (**…**), Enfermera **(…**), y adicionalmente unos grupos comunes en función del ámbito en el que desarrollan su actividad (**…)** si lo requiere su Rol y Categoría, así como grupos específicos que les correspondan según el puesto/especialidad/Servicio y Unidad".*

- Respecto a la trazabilidad y supervisión de accesos se determina:

  "Se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa, contando el Centro a su vez con una serie de auditorías de carácter mensual.

  […]

  *Se realizan auditorías mensuales del fichero de log de accesos a *****SISTEMA.1** mensual que facilita el proveedor CGM.* Se *sigue la metodología establecida a partir de 2019 siguiendo indicación de la Oficina de Seguridad de Sistemas de Información (***DEPARTAMENTO.8) respecto al Indicador "GCP_5.4: Mejorar la gestión de la actividad TIC, del acceso y uso de los sistemas y calidad de la información-- GCP_5.4.1: Grado de proactividad en el control de acceso en la Seguridad de la Información" del Contrato Programa.*

  *Se realiza el análisis automático de los accesos correspondientes al TOP 10 NHCs y TOP 10 profesionales (NHCs y Profesionales con mayor número de registros en la traza del Log de ***SISTEMA.1), para su revisión y se elabora el correspondiente informe.*

  *Adicionalmente y como se recoge en la Instrucción Técnica se realiza un análisis del fichero completo del Log de accesos *****SISTEMA.1**, y se genera una estadística que permite identificar globalmente, posibles incidencias relativas a IPs, perfiles y permisos de acceso, así como un análisis de una muestra aleatoria de líneas de traza del Log, correspondiente a accesos realizados por usuarios que han sido alta o han tenido alguna modificación de perfil, en el período de estudio".*

1. ANÁLISIS DE RIESGOS

Se aporta por el CDPD del ******ORGANISMO.2*** (Anexo VII), el documento que recoge el análisis de riesgos, "e*l cual ha sido elaborado a través de ***HERRAMIENTA.1. La misma trata de un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología *****METODOLOGÍA.1**)."*

Por otro lado, se aporta como Anexo VIII el Plan de Tratamientos de Riesgos (PTR):

"Elaborado por el responsable del Tratamiento (******CENTRO.1***), *en él se incluye un listado de acuerdo a la planificación de las acciones que se deben realizar para mitigar*

los riesgos, una vez se han considerado las amenazas identificadas en el informe resultante del análisis de riesgos y para las que el valor del riesgo es superior a 3.

En dicho PTR, por tanto, quedan detalladas todas esas acciones que serán llevadas a cabo por el propio Centro para mitigar los riesgos resultantes del análisis, siendo las mismas revisadas y aprobadas por el propio Comité de Seguridad de la Información".

Se aporta como Anexo IX el acta del Comité de Seguridad de la Información, fechada el 20 de diciembre de 2023, cuyo orden del día es la revisión y aprobación del PTR elaborado a partir del resultado del análisis de riesgos realizado con ***HERRAMIENTA.1 en 2023, atendiendo al Contrato Programa 2023.

2. ACCESOS A LA HCE POR LOS PROFESIONALES QUE INTEGRAN *EL* ******DEPARTAMENTO.7*** DEL ******CENTRO.1***

El CDPD señala que en ******SISTEMA.1*** se pueden encontrar diferentes roles y categorías:

*"Entre ellos destacan médicos (facultativos y facultativos residentes), farmacéuticos, enfermeros, técnicos medios sanitarios en cuidados auxiliares de enfermería (*TMSCAE*), matronas, administrativos, celadores…, entre otros. Cada perfil, dependiendo de su categoría y su grupo, podrá tener acceso a una información u otra para el correcto desempeño de sus funciones, en aras de garantizar una óptima asistencia sanitaria"*.

Se aporta como Anexo II un extracto del Catálogo de perfiles que incluye los grupos que se asigna a algunos de los roles y categorías de los profesionales con acceso a ******SISTEMA.1.***

En el Anexo I, el ******CENTRO.1*** señala que todos los profesionales que integran el ******DEPARTAMENTO.7*** del ******CENTRO.1*** (Servicio al que pertenecen las facultativas identificadas por la parte reclamante) y que participan en el proceso asistencial (Facultativos, Enfermeros y TMSCAE) acceden a ******SISTEMA.1*** y a la información y documentación disponible en ******SISTEMA.1*** que conforma la Historia Clínica Electrónica para garantizar la correcta prestación de la asistencia. La finalidad de este acceso es estrictamente asistencial.

En cuanto a los equipos que se utilizan en el Servicio, equipos asignados a usuarios y equipos compartidos, en el Anexo I se incluye una tabla donde se identifican:

"(…) La mayoría de los equipos son de uso compartido habitual, esto es debido a que existe una alta rotación de los profesionales por las distintas áreas de trabajo, tanto en jornada ordinaria como de guardia.

*Si bien muchos de los equipos son compartidos, los usuarios inician sesión con un Login y contraseña nominal ***SISTEMA.2, sólo en algunos casos puntuales derivado de las necesidades concretas del servicio, se puede iniciar sesión con un usuario genérico ***SISTEMA.2, con perfil y funcionalidad restringida, lo que no implica que puedan tener acceso de manera genérica al aplicativo* ******SISTEMA.1****, ya que, para acceder a este, sí que es necesario que el acceso sea nominal.*

Todo PC del Hospital tiene una configuración según maqueta sanidad y está incluido en ******SISTEMA.2****. Los equipos están actualizados y se distribuyen políticas ***SISTEMA.2 en el inicio de sesión. Los usuarios inician sesión en los equipos con Login Usuario y* ***(…) ***SISTEMA.2****. En los equipos de zonas concretas y alta rotación* ***(…)*** *se puede iniciar sesión con* ***(…) ***SISTEMA.2 (…)****, que garantiza una*

configuración adaptada a ese puesto de trabajo y los recursos (Impresoras, …) a los que debe tener acceso en horario continuado durante las 24 h, pero igualmente en estos equipos el acceso al aplicativo ******SISTEMA.1*** *es siempre con usuario nominal".*

Como Anexo XII se aportan los flujogramas que se incluyen en el *Procedimiento de la Planificación del Producto en el* ******DEPARTAMENTO.7*** y que describen el proceso ***(…).***

> *"El proceso asistencial representa el continuum clínico desde que un episodio es identificado (como patología o servicio a prestar al paciente) hasta que finaliza o se estabiliza como proceso crónico englobando los niveles de salud. El Sistema de Información Asistencial Integral (*******SISTEMA.1****) es la estructura básica asistencial sobre el que se sustenta toda la actividad clínica que se realiza en cada uno de los ámbitos asistenciales del* ******CENTRO.1****. Este sistema proporciona un entorno de Historia Clínica electrónica que es común para el centro sanitario en cuanto a modelo de datos básicos e interfaz. En el siguiente diagrama de flujo se describe la funcionalidad del programa* ******SISTEMA.1***
>
> *[(…)*
>
> *El profesional del centro accede con usuario y contraseña y autorización según su perfil de usuario a los diferentes módulos".*

3. MECANISMOS PARA QUE NO SE PRODUZCAN ACCESOS INDEBIDOS

A continuación, se relacionan las medidas establecidas en el ******CENTRO.1*** para garantizar el acceso sólo a las personas y a los datos que su función requiere:

- *"Existe una segregación de perfiles para la utilización de la herramienta* ******SISTEMA.1****, teniendo en cuenta el desempeño del trabajo de cada uno de los puestos y limitando a cada usuario el acceso a lo necesario para cumplir con sus funciones, dando por tanto efectivo cumplimiento al principio de mínimo privilegio.*
- *Correcta gestión de usuarios para garantizar que sólo tengan claves de acceso a los SSII los profesionales autorizados y activos, y siempre con los permisos y privilegios que correspondan con las Categorías y Perfiles profesionales y para el desempeño de las funciones y competencias correspondientes que tienen encomendadas.*
- *Restricciones acceso solo desde Equipos con IPs autorizadas en red Salud y que se implementan por las Unidades de Soporte centralizado correspondiente según las medidas de seguridad/organizativas establecidas para el acceso a los SSII y entornos Corporativos como es* ******SISTEMA.1 (…)***
- *En aplicación del Esquema Nacional de Seguridad se registran las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.*
- *Implantación de un proceso de auditorías de carácter mensual a través del fichero del Log de accesos* ******SISTEMA.1,*** *generando una estadística que permite identificar globalmente, posibles incidencias relativas a IPs, perfiles y permisos de acceso, así como un análisis de una muestra aleatoria de líneas*

de la traza del Log, correspondiente a accesos realizados por usuarios que han sido alta o han tenido alguna modificación de perfil, en el período de estudio.

- *Por parte de los empleados se firma un compromiso de confidencialidad, mediante el cual se le informa al trabajador en el momento de formalizar su relación de sus deberes en esta materia.*

  Se aporta como Anexo XIV el Compromiso de confidencialidad y deber de secreto que firman los trabajadores.

- *Política de seguridad a nivel de ***ORGANISMO.1, que prevé medidas organizativas específicas para el mantenimiento de la confidencialidad de la información a la que acceden los trabajadores de la organización.*

- *Iniciativas de Concienciación y Formación en materia de Protección de datos y Seguridad de la Información, Política de acceso SSII, Códigos de Buenas Prácticas, Recomendaciones de Estilo y Código de Conducta, Cláusulas de Confidencialidad y Contratos, Avisos/Recordatorios Normativa en Inicio Sesión en *****SISTEMA.1** pop-up en Inicio sesión equipos con Avisos y Recordatorios en esta materia, pop-up y espacios disponibles en Intranet (con distintos contenidos de interés y utilidad en esta materia de protección de datos y seguridad de la Información)".*

  *En el Anexo XV se muestra la relación de las iniciativas formativas llevadas a cabo en el *****CENTRO.1** en materia de protección de datos y seguridad de la información desde el año 2015.*

  En el Anexo XVI se incluyen las siguientes evidencias:

  - *Correo electrónico enviado por la *****DEPARTAMENTO.8** en marzo de 2022 relativo a medidas preventivas de ciberseguridad que incluye píldora informativa para reforzar el mensaje del cambio voluntario de contraseñas y el apagado de los equipos. Esta píldora se distribuye por correo y adicionalmente, se publica pop-up en la Intranet del *****CENTRO.1** durante 1-2 semanas, en las que también se muestra en el escritorio de los equipos, siguiendo las políticas ***SISTEMA.2.*

  - *Correo electrónico envidado por la *****DEPARTAMENTO.8** en julio de 2023 en el que se informa de la publicación del Boletín de Seguridad de Julio de 2023. Esta comunicación llega a todos los usuarios activos en ***SISTEMA.2 y con correo corporativo *****EMAIL.1.** En el Boletín se incluye, entre otra información en materia de seguridad de la información y protección de datos, píldora formativa de concienciación "¡Haz un uso responsable de la información!*

    *Asimismo, se muestra que la píldora formativa de concienciación relativa a hacer uso responsable de la información se incorpora adaptada en el aviso de inicio de sesión del aplicativo *****SISTEMA.1**:*

    "HAZ UN USO RESPONSABLE DE LA INFORMACIÓN

    LA CONFIDENCIALIDAD DE LOS PACIENTES ES UN BIEN VALIOSO A PROTEGER:

    - *El acceso y uso de datos de pacientes sólo puede realizarse dentro del ámbito asistencial y para el ejercicio exclusivo de tus funciones.*

- *Todos los accesos a los sistemas quedan registrados y los mismos son auditados periódicamente.*
- *Utiliza siempre los canales corporativos para contactar con tus pacientes, y siempre para fines profesionales.*
- *Ten presente que el acceso y uso indebido de la información puede tener consecuencias administrativas y legales".*

En el documento "Uso adecuado de la comunicación electrónica" se presentan los correos electrónicos enviados en fechas 14 de septiembre de 2022 y 16 de agosto de 2023 al personal del ******CENTRO.1*** *recordando la importancia de conocer la normativa vigente aplicable, así como los documentos informativos que se pueden encontrar en la web del* ******ORGANISMO.2*** *o de la* ******CCAA.1****, subrayando que deben utilizarse medios institucionales en el desempeño de la actividad laboral, evitando el uso de recursos particulares como* ******APP.1*** *o correos electrónicos personales.*

- *Medidas Disciplinarias. En caso de identificarse accesos indebidos, y según la normativa vigente respecto a la tramitación de expedientes disciplinarios, en caso de identificarse hechos que pudieran ser constitutivos de faltas graves o muy graves éstos se ponen en conocimiento (… 9***".**

1. ACCESOS A LA HCE DEL RECLAMANTE

DEPARTAMENTO.3 del ******CENTRO.1 pone en conocimiento del CDPD, lo trasladado por la parte reclamante, sospechas de accesos indebidos a su historia clínica por parte de siete compañeras facultativas del ******DEPARTAMENTO.7*** del ******CENTRO.1***, en consecuencia, el CDPD emite informe de asesoramiento (Anexo X), en el que se recoge:

> *"... ante la sospecha de posibles accesos no autorizados a historias clínicas, debe acudirse a la comprobación de las trazas y comunicar averiguaciones a los órganos competentes que deban conocer el asunto en aras de depurar las posibles responsabilidades*."

En consecuencia, ***DEPARTAMENTO.3 del ******CENTRO.1*** solicita al ******DEPARTAMENTO.9*** auditoría e informe, referente a los accesos a la historia clínica de la parte reclamante, por parte de las siete profesionales que identifica (Anexo IV).

El Informe de auditoría de accesos a la HC de la parte reclamante (Anexo II), emitido por ******PUESTO.5*** del ******DEPARTAMENTO.9***, recoge los siguientes resultados, siendo la facultativa 2, ***A.A.A.***:

"DNI		**FECHA**	**Accesos**
(…)		***(…)***	***(…)***
(…)	***(…)***	***(…)***	***(…)***
Facultativa 3			NO (No hay ninguna traza de acceso en ******SISTEMA.1*** de este usuario a esta NHC)

“DNI		**FECHA**	**Accesos**
Facultativa 4			NO (No hay ninguna traza de acceso en ***SISTEMA.1** de este usuario a esta NHC)
Facultativa 5			NO (No hay ninguna traza de acceso en ***SISTEMA.1** de este usuario a esta NHC)
Facultativa 6			NO (No hay ninguna traza de acceso en ***SISTEMA.1** de este usuario a esta NHC)
Facultativa 7			NO (No hay ninguna traza de acceso en ***SISTEMA.1** de este usuario a esta NHC)

En el ANEXO se recoge el detalle correspondiente de la traza de las acciones realizadas en el acceso a la NHC (de la parte reclamante) *para los dos únicos DNI hallados.*

*Estos accesos se realizan desde equipos PCs localizados en el área **(…)**, teniendo en cuenta las Direcciones IPs que aparecen en el log de accesos:*

- *IP *****IP.1** corresponde a PC *****PC.1***
- *IP *****IP.2** corresponde a PC *****PC.2***
- *IP *****IP.3** corresponde a PC *****PC.3”***

En el marco de las actuaciones de investigación, el ******CENTRO.1*** indica la localización de los equipos con estas IPs, (Anexo I) y se comprueba que se encuentran entre los equipos utilizados por los profesionales que integran el ******DEPARTAMENTO.7*** en las distintas áreas de trabajo:

Dirección IP	Nombre – Descripción de Equipo	Localización del equipo	Uso Compartido
******IP.1***	******PC.1 – (…)***	***(…)***	No- Habitual
******IP.3***	******PC.3 – (…)***	***(…)***	SI-Habitual
******IP.2***	******PC.2- (…)***	***(…)***	SI-Habitual

En el Informe elaborado por ***DEPARTAMENTO.3 del ******CENTRO.1*** (Anexo XI), se recogen los resultados de su investigación:

*“Del informe emitido por ***PUESTO.5 de ***DEPARTAMENTO.9 se deduce que:*

(…)

- *Se confirma que la usuaria* **Facultativa 2** *accedió el 23-5-2023 9:45 h. a la historia clínica de* la parte reclamante *y realizó visualización y consulta de datos clínicos desde el ordenador que tiene asignado para uso personal* ***(…)*** *(IP* ******IP.1****).*

(…) “)

En relación con la justificación de la finalidad de estos accesos a la HCE de la parte reclamante, ******CENTRO.1*** traslada que **estos accesos no están justificados** al no corresponder a finalidad asistencial alguna dirigida a la parte reclamante.

1. OTRAS ACTUACIONES DEL ****CENTRO.1*

DEPARTAMENTO.3 del ******CENTRO.1 traslada la reclamación y los informes disponibles al ******SERVICIO.1*** del ******ORGANISMO.2***, para que valore el alcance de la falta, dado que considera que los hechos manifestados por la parte reclamante y verificados por el ******CENTRO.1*** podrían ser objeto de sanción disciplinaria, quien acuerda ***(...)*** a la facultativa ***A.A.A.*** Asimismo, ***DEPARTAMENTO.3 del ******CENTRO.1*** remite respuesta a la parte reclamante.

Como resultado de la investigación y con relación al asunto que nos trata:

- El ******CENTRO.1*** informa que, todos los profesionales que integran el Servicio al que pertenece la facultativa identificada por la parte reclamante, participan en el proceso asistencial y que, para garantizar la prestación de la asistencia sanitaria, acceden al aplicativo ******SISTEMA.1***, que es la aplicación de Historia Clínica Electrónica (HCE) que se utiliza por ***ORGANISMO.1 de la ******CCAA.1***.

- En el informe elaborado por ***DEPARTAMENTO.3 del ******CENTRO.1*** se recoge que ***A.A.A.*** accedió a la historia clínica de la parte reclamante, de forma injustificada, al no corresponder a finalidad asistencial alguna; y lo hizo desde el ordenador que tiene asignado para uso personal en el Servicio ***(…)***.

QUINTO: Con fecha 21/02/2025 la Presidencia de la AEPD acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por las presuntas infracciones de los artículos 9 y 6.1 del RGPD, ambas tipificadas en el artículo 83.5.a) del RGPD.

SEXTO: Notificado el citado acuerdo de inicio 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), la parte reclamada presentó escrito de alegaciones en fecha 10/03/2025, en el que, en síntesis y por lo que interesa en el presente procedimiento sancionador, manifestaba lo siguiente:

- El acuerdo de inicio no ha tenido en cuenta el resultado de las investigaciones realizadas por los mismos hechos por el ******ORGANISMO.2*** en el marco del ***(…)*** que le fue abierto por el que quedaría probado que no pudo demostrarse que el acceso a la historia clínica de la parte reclamante se realizara por ***A.A.A.,*** sino únicamente a través de su usuario. Subraya que tras el

mencionado procedimiento se le impuso una ***(…)***, contra el criterio contenido en la ***(…),*** sin que, en ningún caso, quedara probaba la autoría en el acceso***.***

- Además, insiste en la imposibilidad física del acceso imputado, dado que, en el momento en que se produjeron los hechos, se encontraba atendiendo una urgencia. Asegura que este elemento se contiene en la ***(…).***

A la vista de lo anterior, solicita el archivo del procedimiento sancionador, o en su defecto, la disminución de la sanción fijada inicialmente.

Junto a su escrito de alegaciones presenta, entre otra documentación:

- ***(…) ***CENTRO.1*** en la que se indica:

> ***"(…)***
>
> *Que el día 23 de mayo de 2023 en diferentes horarios 9.45 horas, 9.46 horas y 9.47 horas se accede desde su usuario* ***(…)*** *al número de historia clínica* ***(…)***

(…)
- Justificante de presentación de recurso contencioso-administrativo contra la mencionada ***(…)*** presentada por ***A.A.A.***
- Alegaciones efectuadas por ***A.A.A.*** en el marco del ***(...).***

SÉPTIMO: El 06/05/2025, tuvo entrada en la AEPD nuevo escrito de ***A.A.A.*** en el que comunica lo siguiente:

"En el día de ayer se me ha notificado la ******SENTENCIA.1,*** que estima el recurso contencioso administrativo interpuesto por mí frente a las resoluciones que le sancionaron en el procedimiento de que trae causa el expediente ante esta Agencia, a saber:

- (…)

(…)

La sanción se anula por falta de culpabilidad, acreditando que cuando se produjeron los hechos objeto de este expediente ante la Agencia, me encontraba atendiendo una emergencia clínica en otra unidad (…)

La sentencia declara expresamente probado que es otra persona la que, aprovechando mi ausencia por estado de necesidad, entra en mi despacho, accede a mi ordenador (…)

La Sentencia (…):

- *Anula la sanción que se me impuso por el* ******ORGANISMO.2.***
- *Declara probado que yo no he accedido a la historia clínica de B.B.B.**.***
- *Declara igualmente probado que la sesión de mi ordenador quedó abierta por causa de estado de necesidad (porque hube de atender una emergencia sanitaria con grave riesgo para la vida de un paciente) y aprecia la eximente completa anulando la sanción por falta de culpabilidad.*

Y, en su razón, archive sin más este procedimiento sancionador"

Junto a su escrito aporta copia de la ***SENTENCIA.1 en la que se determina lo siguiente (el subrayado es de la AEPD):

(…) SÉPTIMO: Pues bien, de la prueba practicada y consistente en documental, expediente administrativo y testifical (…), en el presente caso, resulta sumamente dudoso poder admitir y afirmar como hace la Administración demandada la existencia de un incumplimiento de las funciones encomendadas a la funcionaria ahora demandante, o bien, un incumplimiento de las normas reguladoras del servicio sanitario a que está sometido o vinculado. En otras palabras, resulta cuestionable estimar infringido el artículo 72.3.c) de la Ley 55/2003, de 16 de diciembre, lo que podría conducir a considerar vulnerado el principio de tipicidad de la infracción (artículo 27 de la Ley 40/2015), por cuanto la parte recurrente actuó en todo momento y así ha quedado acreditado ninguna intención o falta de diligencia que integre el concepto de culpabilidad requerido para que concurra la imputación y su consecuente sanción, máxime cuando ello es consecuencia precisamente por cumplir con sus funciones ***(…)*** *y haberse acreditado que en el momento de los hechos, y ante la emergencia médica a la que tuvo que atender, la sesión de su ordenador quedó iniciada por cumplimiento de un deber inexcusable cual era la vida de una persona, por tanto concurriría una causa de exención de la responsabilidad (art. 20.5 del CP), el estado de necesidad. Asimismo, junto a tal situación de emergencia también realizó dos actuaciones más en ***DEPARTAMENTO.7****,* *como ha quedado acreditado de la documental y testifical. A ello se une que si la parte recurrente estaba en ***DEPARTAMENTO.7 (desde las 9.45 y 9.47 horas), atendiendo tal emergencia y las dos actuaciones, tal y como ello ha quedado acreditado, de documental y de la testifical depuesta, la cual no ha incurrido en contradicción, o dubitación, siendo su relato coherente, y espontáneo, declaración que ha resultado corroborada por otros medios de prueba, en particular por los documentos del expediente administrativo, y siendo el ordenador con dirección* ***IP ***IP.1*** *el asignado a la parte recurrente* ***(…),*** *no se ha acreditado que sea la parte recurrente la persona que estaba en su ordenador entre las 9:44:01 y las 9:47:30 accediendo a la historia clínica de B.B.B.****,*** *de lo que además cabe decir, dicho sea de paso, que siendo el despacho y ordenador de uso personal para la persona ejerciente y no estando la parte recurrente en dichas horas en los mismos, por alguna persona se accedió a dicho lugar y ordenador (…) Por tanto, de la prueba practicada, los hechos que se imputan a la parte recurrente ni son constitutivos del tipo infractor que le ha sido aplicado, ni queda acreditada su intencionalidad o su culpabilidad, lo que además refuerza el hecho de que el Instructor formuló propuesta de sobreseimiento y consiguiente archivo de las actuaciones derivadas del expediente incoado(…)*

(…) ESTIMO el recurso contencioso-administrativo (…) anulo y dejo sin efecto por no ser conforme a Derecho (…) Notifíquese esta Sentencia a las partes personadas haciéndoles saber que es FIRME y NO cabe contra ella recurso ordinario de apelación de conformidad con lo establecido en el artículo 81 de la LJCA".

OCTAVO: Con fecha 5 de septiembre de 2025 se formuló propuesta de resolución, proponiendo:

- *Que, por la Presidencia de la Agencia Española de Protección de Datos, se proceda al **ARCHIVO** del procedimiento iniciado contra **A.A.A.**, con NIF *****NIF.1**, por infracción del artículo 9 del RGPD, tipificada en el artículo 83.5 a) del RGPD.*

- *Que, por la Presidencia de la Agencia Española de Protección de Datos, se proceda al **ARCHIVO** del procedimiento iniciado contra **A.A.A.**, con NIF *****NIF.1**, por infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5 a) del RGPD.*

NOVENO: En fecha 9/09/2025 ***A.A.A.*** presentó escrito ante esta Agencia por el que manifiesta su conformidad con el sentido de la propuesta de resolución.

HECHOS PROBADOS

PRIMERO: El 23 de mayo de 2023 sobre las 9:45 horas se accedió a la historia clínica de ***B.B.B., ***PUESTO.1*** del ******CENTRO.1,*** desde la dirección IP ******IP.1,*** vinculada al ordenador asignado ***(…)*** a ***A.A.A.***

Asimismo, el acceso se realizó con el usuario correspondiente a ***A.A.A.***

SEGUNDO: El 23 de mayo de 2023 entre las 9:45 hasta las 9:47 horas, mientras se producía el acceso a la mencionada historia clínica desde su ordenador y su usuario, ***A.A.A.*** se encontraba en ***DEPARTAMENTO.7 atendiendo una emergencia sanitaria, tal y como consta probado en la ***SENTENCIA.1 que asegura que *"no estando **(…)** en dichas horas en los mismos, por alguna persona se accedió a dicho lugar y ordenador".*

TERCERO: No consta la identidad de la persona que accedió a la historia clínica de *B.B.B.* el 23 de mayo de 2023 desde la dirección IP ******IP.1,*** y con el usuario asignado a ***A.A.A.***

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para resolver este procedimiento 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

Cuestiones previas

El artículo 4.1 del RGPD define dato personal como "*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*"

Por su parte, el apartado 2 del mismo precepto define el tratamiento de datos como "*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*;"

Finalmente, el apartado 7 define al responsable del tratamiento o responsable como "*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;"*

Por su parte, las Directrices del CEPD 07/2020 destacan que el concepto de responsable del tratamiento es un concepto funcional, siendo necesario establecerlo en virtud de sus actividades concretas en el caso analizado y no en función de una designación formal que pueda figurar en un contrato u otra documentación:

> *"12. Los conceptos de «responsable del tratamiento» y «encargado del tratamiento» son conceptos funcionales: su objetivo es asignar responsabilidades en función del papel real de cada parte. Esto implica que la condición jurídica de «responsable del tratamiento» o «encargado del tratamiento» de los participantes debe establecerse en principio en virtud de sus actividades concretas en una situación determinada y no en función de la designación formal de un participante como «responsable del tratamiento» o «encargado del tratamiento» (p. ej., en un contrato).Esto implica que la asignación de la función de responsable o encargado debe derivar normalmente de un análisis de los hechos o circunstancias del caso y, en consecuencia, no es negociable." (El subrayado es de la AEPD).*

Asimismo, las referidas Directrices del CEPD 07/2020 abogan por una interpretación amplia del concepto de responsable del tratamiento con el fin de promover una protección eficaz y completa de los interesados. En este sentido, prevén:

> *"14. Puesto que el objetivo último de la atribución de la función de responsable del tratamiento es garantizar la responsabilidad proactiva y una protección eficaz e integral de los datos personales, el concepto de «responsable» debería interpretarse de un modo suficientemente amplio, de manera que promueva, en la medida de lo posible, una protección eficaz y completa de los interesados , con el fin de garantizar la plena eficacia del Derecho de la Unión en materia de protección de datos, evitar lagunas y prevenir las posibles elusiones de la normativa, sin que todo ello suponga una merma de las atribuciones del encargado del tratamiento." (subrayado de la AEPD).*

A lo ya expuesto hasta el momento, cabe añadir que dichas Directrices del CEPD destacan:

> *"20. (…) El responsable del tratamiento es quien decide determinados aspectos esenciales del tratamiento de los datos. La responsabilidad del tratamiento puede establecerse en la normativa o deducirse de un análisis de los hechos o las circunstancias del caso. Es necesario dirigir la atención a las actividades de tratamiento concretas de que se trate y comprender quién las determina. Para ello, primero deben examinarse las siguientes cuestiones: «¿por qué tiene lugar el tratamiento?» y «¿quién ha decidido que debe llevarse a cabo el tratamiento para un fin concreto?»."*

En relación con lo anterior, conviene señalar que, en principio, no existen limitaciones hacia el tipo de ente que puede asumir la condición del responsable del tratamiento (ya sea una persona física o jurídica, autoridad pública, servicio u organismo, de acuerdo con el artículo 4.7 del RGPD).

Sin perjuicio de lo anterior, con carácter general, el responsable del tratamiento en el sentido del RGPD suele ser 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 de datos. El hecho de que esa 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.

En estos términos se ha pronunciado el CEPD en las mencionadas Directrices:

> *"17. (…) en principio, no existen restricciones en relación con el tipo de ente que puede asumir la función de responsable del tratamiento. Puede ser una organización, pero también un individuo o un grupo de individuos. Sin embargo, en la práctica, quien actúa como responsable del tratamiento en el sentido del RGPD suele ser la propia organización como tal y no una persona dentro de esta (p. ej., el director general, un empleado o un miembro del Consejo). Por lo que respecta al tratamiento de datos dentro de un grupo de empresas, debe prestarse especial atención a la cuestión de si un establecimiento puede estar actuando como responsable o encargado del tratamiento, p. ej., al tratar datos en nombre de la sociedad matriz.*
> *18. En ocasiones, las empresas y los organismos públicos nombran una persona concreta a la que hacen responsable de las actividades de tratamiento. Aun cuando se nombre a una persona física concreta para*

> *garantizar el cumplimiento de la normativa sobre protección de datos, esta no será el responsable del tratamiento, sino que actuará por cuenta de la persona jurídica (empresa u organismo público), que, en última instancia, responderá, en calidad de responsable del tratamiento, de las posibles infracciones de la normativa. En esta misma línea, aunque un departamento o unidad de una organización ostente la responsabilidad operativa de asegurar la conformidad de determinada actividad de tratamiento, ello no significa que dicho departamento o unidad (en lugar de la organización en su conjunto) devenga responsable del tratamiento".*

Esto implica que, con carácter general, los empleados que disponen de acceso a datos personales dentro de una organización no tienen la consideración de responsables ni de encargados del tratamiento, sino de "personas que actúan bajo la autoridad del responsable o del encargado" en el sentido previsto en el artículo 29 del RGPD, que señala:

> *"El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros".*

No obstante, existen excepciones a esta regla general como consecuencia de ese "concepto funcional" de responsable del tratamiento fijado por el RGPD y de la necesidad, por tanto, de realizar una interpretación amplia del concepto del responsable del tratamiento, determinado por la actividad material realizada por una persona física o jurídica en una situación concreta. Así en aquellos supuestos en los que un empleado realizara tratamientos de datos personales para sus propios fines, excediéndose de manera indebida de las funciones que tuviera encomendadas, no podrá considerarse que estén actuando "bajo la autoridad" del responsable, deviniendo responsables por sí mismos, siempre que la organización hubiera adoptado todas las medidas técnicas y organizativas destinadas a evitar este riesgo.

En este sentido se pronuncian las Directrices 07/2020 del CEPD:

"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, ***A.A.A. (…)*** y presta sus servicios ***(…)*** en ******DEPARTAMENTO.7*** del ******CENTRO.1.*** Presta sus servicios como facultativa especialista, realizando las actividades que le son propias en el marco de su relación laboral con la mencionada

organización o entidad. En este sentido, en tanto que personal sanitario y de conformidad con el artículo 16.5 de la LAP, tiene acceso a las historias clínicas de sus pacientes.

No obstante, en caso de que ***A.A.A.*** realizara accesos a historias clínicas de personas con los que no existe relación asistencial alguna, ni relación médico-paciente, así como contraviniendo las instrucciones del ******CENTRO.1,*** podrían suponer un tratamiento de datos personales para sus propios fines, extralimitándose de manera ilícita en el ejercicio de las funciones atribuidas por el ******CENTRO.1***, pasando a determinar los medios y fines del tratamiento de datos personales y deviniendo responsable del mismo.

III

Contestación a las alegaciones al acuerdo de inicio

A la vista de las alegaciones realizadas por ***A.A.A.*** al acuerdo de inicio y revisada la documentación aportada, se comprueba que no ha quedado acreditado que el acceso a la historia clínica de la parte reclamante el 23 de mayo de 2023 se produjera por ***A.A.A.***

Así, si bien el acceso se produjo desde la IP y el usuario vinculado a la parte reclamada, esta se encontraba en un lugar distinto al que se produjeron los hechos en el momento en que estos tuvieran lugar. Así se recoge por la ***SENTENCIA.1**,* aportada por ***A.A.A.,*** que señala que se ha probado que la parte reclamada se encontraba atendiendo una emergencia médica, sin que se haya identificado a la persona que accedió a su despacho y a su ordenador para consultar la historia clínica de la parte reclamante.

Por otra parte, la ******RESOLUCIÓN.1,*** aportada por la parte reclamada y anulada posteriormente por la sentencia anteriormente mencionada, sancionaba a ***A.A.A.*** por el incumplimiento de buenas prácticas respecto al cierre de su sesión de usuario y la activación del bloqueo de las pantallas al ausentarse de un ordenador, sin que hubiese quedado acreditado, por tanto, ***(…)***, que ***A.A.A.*** fuera quien efectivamente accedió a la historia clínica en cuestión.

Procede, en consecuencia, estimar las alegaciones de la parte reclamada por las que solicita el archivo del procedimiento sancionador en la medida en que no han quedado acreditados los hechos contenidos en el acuerdo de inicio.

IV

Tratamiento de datos personales de categoría especial. Artículo 9 del RGPD

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."

El artículo 4.15 del RGPD define "*datos relativos a la salud*" como "*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*"
Los datos de salud se encuentran dentro de las "categorías especiales de datos", también conocidos como datos sensibles, por lo que merecen una protección reforzada y sólo se podrán tratar, es decir, almacenar, transmitir o revelar, entre otras formas de tratamiento, bajo ciertas condiciones y con determinadas garantías y ello se debe a que tienen una incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona. Para el tratamiento de estos datos de categoría especial, se precisa en primer lugar, de la concurrencia de una causa de levantamiento de la prohibición del art. 9.2. RGPD y también como para cualquier tratamiento, de una base de legitimación del art. 6.1 RGPD.

La finalidad de la historia clínica es fundamentalmente asistencial. Puede acceder a la historia clínica, el profesional sanitario o el equipo directamente implicado en la asistencia al paciente, o aquellos que sean consultados por éste, con la finalidad de mejorar la atención terapéutica.

El acceso a la historia clínica está limitado, no cualquier profesional y ante cualquier circunstancia puede acceder. Tanto el personal sanitario, como otros profesionales, pueden acceder a ella únicamente para el desempeño de sus funciones, sin que puedan revelar a terceros los datos a los que tienen acceso. Las posibilidades para acceder a los datos de la HC son distintas según el tipo de función profesional y de la finalidad del acceso a dichos datos. En todo caso, es preciso que concurra alguna de las causas de levantamiento de la prohibición del tratamiento de datos de categorías especiales del artículo 9.2 RGPD. Las excepciones, a la prohibición del tratamiento de datos de salud establecida por el artículo 9.1, vienen determinadas en el artículo 9.2 del RGPD. Es decir, es necesario que concurra alguna de las premisas establecidas en el mencionado artículo para que se pueda llevar a cabo el tratamiento de datos de salud, por ejemplo. Estas excepciones han de interpretarse de manera restrictiva, tal y como se desprende de los considerandos del 51 al 56 del RGPD.

V
Licitud del tratamiento. Artículo 6 del RGPD.

El artículo 6.1 del RGPD establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

VI
Presunción de inocencia

La Sentencia del Tribunal Supremo de 29 de enero de 1994, recogiendo una línea jurisprudencial consolidada, advierte que *"tanto el T.C. (STC de 8.6.81 y 3.10.83, entre otras), como el T.S. (SSTS de 26.4. y 17.7.82) han perfilado una doctrina en materia de derecho sancionador, de la que merecen destacarse como líneas maestras las siguientes: (…)*

2º.- En materia de Derecho Administrativo sancionador son de aplicación los principios generales del Derecho Penal, coincidentes sustancialmente con los principios esenciales reflejados en el art. 24 CE. en materia de procedimiento, y han de ser aplicables en la medida necesaria para preservar los valores esenciales que se encuentran en la base del precepto y la seguridad jurídica que garantiza el art. 9 CE

3º.- Lógica consecuencia de todo ello es que la presunción de inocencia, proclamada en el párrafo 2º de tal precepto, supone que la carga probatoria de los hechos en que se basa recae sobre la parte que los imputa, y por otra parte, que el principio de tipicidad exige también para su aplicación la plena concordancia de los hechos imputados en las
previsiones prácticas aplicables al caso."

Por tanto, para extrapolar al Derecho Administrativo sancionador los principios de la esfera punitiva, ha de exigirse que la conducta infractora reúna los requisitos que en el ámbito Penal se establecen para los delitos y faltas.

En consecuencia, la responsabilidad administrativa no puede asentarse en una ausencia de certeza plena sobre los hechos imputados, pues toda sanción ha de apoyarse en una actividad probatoria de cargo o de demostración de la realidad de la infracción que se reprime, sin la cual la represión misma no es posible (Sentencias del Tribunal Constitucional de 11 de marzo de1985, 11 de febrero de 1986, y 21 de mayo de 1987), y, ello, porque al beneficiar la presunción de inocencia al administrado en el ámbito de la potestad sancionadora de la Administración (de conformidad con el artículo 24.2 de la Constitución), ha declarado la Sentencia del Tribunal Constitucional

de 8 de marzo de 1985 que dicha presunción no puede entenderse reducida al estricto campo del enjuiciamiento de conductas presuntamente delictivas, sino que debe presidir también la adopción de cualquier resolución o conducta, de las personas de cuya apreciación derive un resultado sancionador o limitativo de sus derechos, comportando el Derecho a la presunción de inocencia que la sanción esté 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, toda vez que el ejercicio del *"ius puniendi",* según la Sentencia del Tribunal Constitucional de 26 de abril de 1990,está condicionado en sus diversas manifestaciones por el artículo 24.2 de la Constitución al juego de la prueba y a un pronunciamiento contradictorio en el que puedan defenderse las propias posiciones.

El principio de Presunción de Inocencia es un Derecho Fundamental reconocido en el artículo 24.2 de la Constitución Española.

2. *Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.*

Según reiterada Jurisprudencia, la presunción de inocencia exige una valoración de la suficiencia de la prueba de cargo, siendo necesario que el fallo condenatorio se apoye en verdaderos actos de prueba y no en meras especulaciones.

Por su parte el principio "*in dubio pro reo"* en el Ordenamiento Jurídico Español significa que *"toda persona es inocente hasta que se demuestre lo contrario"*, esto significa que si existen dudas acerca de la culpabilidad de una persona, en un delito, los Jueces deberán declararla inocente o no culpable.

No obstante, la Jurisprudencia del Tribunal Supremo indica que el principio "*in dubio pro reo",* no tiene carácter orientativo en la valoración de la prueba. Por lo tanto, solo ha de aplicarse cuando no exista seguridad acerca de la culpabilidad del acusado a la vista de las pruebas.

Es conocido que el Tribunal Supremo (vid. STS, 2ª, nº 459/2018, de 10 de octubre), modificando su anterior jurisprudencia, entiende que el principio *in dubio pro reo* forma parte del Derecho a la presunción de inocencia. La presunción de inocencia supondría la exigencia ineludible de concurrencia de prueba de cargo lícita y válida suficiente para dotar de certeza a la tesis acusatoria. Por su parte, el principio *in dubio pro reo* actuaría en un momento posterior del estadio de la valoración probatoria, una vez superado por la acusación el umbral de la presunción de inocencia del acusado. De alguna forma, la presunción de inocencia haría referencia a la existencia de prueba de cargo objetivamente convincente, mientras que in *dubio pro reo* se aplicaría a aquellos casos en los que el Tribunal, a pesar de existir esa prueba de cargo objetivamente suficiente para fundar una condena desde la perspectiva de la presunción de inocencia, albergara alguna duda subjetiva sobre la culpabilidad del acusado. En esos casos, se entiende por nuestra Jurisprudencia que, si el Tribunal mantiene sus dudas y

su *"falta de convicción",* debe, en todo caso, absolver al acusado. Y si a pesar de ello le condena y hay constancia en la Sentencia de esas dubitaciones, la resolución debe ser revocada o casada en vía de recurso.

VII
Conclusión

En el presente caso, a la vista de las alegaciones realizadas al acuerdo de inicio y revisada la documentación obrante en el expediente, no ha podido acreditarse que el 23 de mayo de 2023 ***A.A.A., (…),*** accediera a la historia clínica de ***B.B.B..*** Y es que, aun cuando el acceso se produjera desde la IP de su ordenador y con su usuario, esta se encontraba atendiendo una emergencia sanitaria en el momento de los hechos.

(…)

En consecuencia, no se aprecia una conculcación de los artículos 9 y 6 del RGPD, siendo procedente el archivo del procedimiento sancionador iniciado contra la parte reclamada.

Por lo tanto, de acuerdo con la legislación aplicable, por la Presidencia de la Agencia Española de Protección de Datos, SE RESUELVE:

PRIMERO: ARCHIVAR el procedimiento sancionador iniciado contra ***A.A.A.*** con NIF******NIF.1*** por:

- La presunta infracción del artículo 9 del RGPD, tipificada en el artículo 83.5 a) del RGPD.

- La presunta infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5 a) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a ***A.A.A.*** con NIF******NIF.1***.

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 artículo 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 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.

Finalmente, se señala que conforme a lo previsto en el artículo 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://sedeaepd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el artículo 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.

938-180725

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