Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR POR INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Resolución	RPS-2024/029
Procedimiento Sancionador	PS-2023/031
Entidad incoada	Dirección General de Asistencia Sanitaria y Resultados en Salud (Servicio Andaluz de Salud)
Motivo de la reclamación	Notificación de una brecha de seguridad de datos personales por pérdida de un disco duro externo del Servicio de Admisión y Documentación Clínica del Hospital *[nombre del hospital]*.
Artículos afectados	5.1.f) y 32 RGPD

Abreviaturas:
RGPD. 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 (Reglamento general de protección de datos)
LOPDGDD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LOPDP. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
LTPA. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía
ESTATUTOS CTPDA. Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre.
LPAC. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
LRJSP. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
ENS. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

ANTECEDENTES

Primero. Notificación de la brecha de seguridad.

1. El 20 de julio de 2023 tuvo entrada en el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) una notificación relativa a una brecha de seguridad de datos personales suscrita por el delegado de protección de datos del Servicio Andaluz de Salud, en aplicación de lo establecido en el artículo 33 del Reglamento (UE) 2016/679 General de Protección de Datos1 (RGPD).

2. En particular, en la notificación se informa, entre otros, de los siguientes aspectos sobre la brecha. La brecha fue detectada inicialmente el 30/05/2023, fue registrada en el sistema informático interno del SAS el 11/07/2023 y notificada al Consejo el 21/07/2023.

Trae causa de la misma la pérdida de un disco duro externo del Servicio de Admisión y Documentación Clínica del Hospital *[nombre del hospital]*.

En dicho dispositivo se almacenaba información del "Conjunto Mínimo Básico de Datos (CMBD)" de los últimos nn años, de aproximadamente nnn episodios. El dispositivo no contaba con ninguna medida de seguridad, si bien quedaba custodiado bajo llave en un cajón de un despacho. Dicho despacho no disponía de sistema de videovigilancia.

Consecuencia de la brecha de seguridad, se han visto afectados datos básicos y relativos a la salud de pacientes, estimándose el número de personas afectadas entre nnnn y nnnn personas. No se descarta que alguna de las personas afectadas residan en otros países.

Se determina que el impacto potencial sobre los afectados es la "pérdida de control sobre sus datos", sin que sea posible estimar la existencia de consecuencias al no tener constancia de la existencia de robo, ni de su autor en su caso.

Las medidas consideradas para minimizar el impacto de la brecha han sido informar a los afectados mediante publicación en la web del centro sanitario afectado, así como denunciar la desaparición del dispositivo a las fuerzas de seguridad.

3. De acuerdo con la información proporcionada en la web del SAS, el conjunto mínimo básico de datos de Andalucía (CMBD Andalucía) es:

"un registro administrativo que contiene un conjunto de variables clínicas, demográficas y administrativas que resumen lo acontecido a un usuario en un episodio de asistencia hospitalaria. Proporciona información básica sobre el usuario, sobre el centro y unidad que lo atienden y sobre su proceso asistencial."

Segundo. Acuerdo de inicio de procedimiento sancionador. (arts. 68 LOPDGDD; Art. 64 LPAC).

1. El 21 de agosto de 2023 el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra la Dirección General de Asistencia Sanitaria y Resultados en Salud (Servicio Andaluz de Salud, con NIF *[NNNNN]*), por la presunta infracción del artículo 5.1.f), tipificada en el artículo 83.5 RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) LOPDGDD. Y por la presunta infracción del artículo 32.1 RGPD, tipificada en el artículo 83.4 RGPD, y calificada como grave a efectos de prescripción en el artículo 73.f) LOPDGDD.

2. Notificado el acuerdo de inicio al órgano reclamado el 22 de agosto de 2023, éste presentó alegaciones en las que, en síntesis, manifestaban lo siguiente:

   a) Escrito de la Dirección General de Asistencia Sanitaria y Resultados en Salud:

   "(...)En respuesta a su oficio de 22/08/2023 dirigido a esta Dirección General, en relación con el Acuerdo de inicio de oficio del procedimiento sancionador dictado por el Director del Consejo de

Transparencia y Protección de Datos de Andalucía contra la Dirección General de Asistencia Sanitaria y Resultados en Salud (Servicio Andaluz de Salud) (PS-2023/031), por el motivo:

"Brecha de seguridad digital en el Hospital [nombre del hospital]"

Se solicitó información al respecto de las cuestiones planteadas a la Dirección-Gerencia del centro implicado, emitiendo el mismo, el informe de Alegaciones que se adjunta.".

b) Escrito de la Dirección- Gerencia del Hospital *[nombre del hospital]*, de 28 de septiembre de 2023, en el que se indica:

"(...)INFORME SOBRE SUSTRACCIÓN DE DISCO DURO EN EL SERVICIO DE CALIDAD Y DOCUMENTACIÓN SANITARIA (Incidencia nº nnnnn de Ayuda Digital)

En el año aa, con objeto de tener una copia de seguridad de los datos de dicho año, por el Servicio de Calidad y Documentación Clínica, se solicitó al Servicio de Informática la adquisición de un disco duro externo, accediéndose a la petición, facilitándose un disco duro externo marca nnn, utilizándose para la finalidad antes expuesta. Dicho disco duro es utilizado por los médicos documentalistas y el jefe de grupo.

El mencionado disco duro se guardaba en una dependencia del Servicio de nnn, donde la entrada está restringida a los profesionales que prestan servicios en el mismo. *[...]*. Además, dicho disco duro se encontraba depositado en el interior de un armario con llave, junto a otro material de trabajo, guardándose la llave en *[...]* accediéndose a él, previa petición de la llave por parte de los referidos profesionales de la Unidad que lo requirieran.

Por otro lado, existe una cámara de seguridad a la entrada del Servicio, que sólo graba el acceso al mismo, mas no el interior, donde se desarrolla el trabajo habitual, al no estar permitido.

A principios de febrero de aa, se envió a Servicios Centrales del SAS el Conjunto Mínimo Básico de Datos (CMBD) completo del año anterior. Este archivo está en formato nnn conteniendo datos numéricos (como fecha de nacimiento, código postal, ...) y alfanuméricos (como NUHSA,· datos clínicos codificados con CIE-10, ...), en el que no se identifican con nombre y apellidos a los usuarios y es imposible relacionar los datos que allí aparecen con un nombre de usuario, para ello necesitarían otra base de datos y cruzar la información. En dicha fecha se realizó una copia de dicho archivo en nnn (espacio de almacenamiento informático en entorno del Hospital *[nombre del hospital]* y en el disco duro anteriormente mencionado.

A finales de mayo de aa, en el Servicio de Documentación Clínica se procede a efectuar otra copia de seguridad del CMBD en el disco duro, evidenciando que no se encontraba en el armario donde se guardaba. Inmediatamente se comunicó la incidencia a la Jefatura de Servicio en primer lugar, y posteriormente a los profesionales del Servicio de Documentación Clínica, por si hubiera sido utilizado por los profesionales para otros fines, descartándose esta posibilidad durante el mes de mm. El día dd el Dr. *responsable*, inicia el mecanismo de comunicación institucional a través de Ayuda Digital (número de incidencia nnn) y al Responsable de Seguridad TIC, al tratarse de una brecha de seguridad de protección de datos por sustracción de disco duro externo con datos del CMBD del HURS. Por otro lado, el mm se comunicó a los *[responsables jerárquicos]*, constando la presentación de denuncia en la Comisaría de Policía por la sustracción del dispositivo de almacenamiento de datos el día *[dd/mm/aa]* (ANEXO 1).

Las **medidas y recursos existentes** con carácter previo a la aparición de la brecha:

1. Desde la Unidad de Formación de SS.CC. del SAS se ha puesto a disposición de todos los profesionales distintas acciones formativas en materia de seguridad y protección de datos personales que contemplan medidas de prevención de situaciones como la ocurrida.

2. En la web del SAS, existe un espacio dedicado expresamente a ofrecer información respecto de los principales tratamientos de datos personales existentes, junto con información complementaria en forma de preguntas frecuentes que abarca directamente las brechas en la seguridad de los datos personales. De manera similar existe un espacio dedicado a la seguridad TIC.
3. Se dispone de una herramienta corporativa desde la que cualquier trabajador/a pueden registrar las brechas de seguridad.
4. Existe personal especializado en materia de seguridad y protección de datos con capacidad para asesorar a quien lo necesite.
S. Se dispone de medios de almacenamiento alternativos a los discos duros externos con capacidad para alojar la información que precisen los distintos servicios, así como herramientas para facilitar el teletrabajo.
Gran parte de estas medidas se encuentran detalladas en el Anexo 3.
Las **medidas recomendadas** e implementadas desde su comunicación se realizaron de forma escalonada:
1. D. [Nombre del Responsable de seguridad TIC, el *[dd/mm//aa]* analizó la situación, nos informó de los aspectos facilitadores del incidente y nos dio pautas de cómo proceder para tener datos seguros:
• Evitar el uso de discos externos para tener información del hospital, especialmente de carácter personal, indicándonos a su vez que existen reposiciones en Consigna, Ficheros Junta e incluso correo electrónico corporativo que nos permite trabajar puntualmente con cierta información. En el caso de que estuviera justificado el uso de un disco duro, deberían implementarse medidas de seguridad que mitiguen el riesgo, como sería el cifrado del dispositivo.
• Recomendación de utilizar sólo las herramientas informáticas de las que disponemos: nnn y nnn.
2. D. [Nombre del Jefe de Servicio TIC], el *[dd/mm//aa]*, recomendó el uso de repositorios que posee el HURS para almacenamiento de este tipo de datos y el cifrado de discos externos si fuera necesario su uso.
3. D. [Nombre del Subdirector Provincial de Tecnologías de la Información y Comunicación] el *[dd/mm//aa]* refuerza las medidas anteriormente citadas.
4. Desde Ayuda Digital la incidencia ha sido tratada por D. [Nombre de miembro de Ayuda Digital], el cual el *[dd/mm//aa]* se puso en contacto con el Servicio de Documentación Clínica notificando la comunicación de esta brecha de seguridad al Consejo de Transparencia y Protección de Datos de Andalucía, y por otro lado recomendando:
• Denunciar la sustracción del disco duro a la Policía Nacional.
• Notificación a los ciudadanos mediante un modelo de documento (Anexo 2), siguiendo las indicaciones que establece el artículo 34 del RGPD de la información.

Las **medidas adoptadas** a raíz del evento:
1. Comunicación vía administrativa a Ayuda Digital (*[dd/mm//aa]*).
2. Adoptar las medidas aconsejadas por Subdirección Provincial de Tecnologías de la Información y Comunicación, por el Responsable de Seguridad de la Información del Hospital *[nombre del hospital]*, y por las de "Ayuda Digital" desde la fecha de su recomendación :
- Ubicar los datos que manejamos sólo en un entorno seguro como es nnn.
- No utilizar el disco duro para copias de datos de usuarios ni cualquier información de carácter personal.
3. Formular denuncia en la Comisaría de Policía por la sustracción del disco duro, presentándose la misma con fecha *[dd/mm//aa]*.

4. Comunicación a la ciudadanía en la web del centro (Anexo 2)"

A dicha documentación se acompañaba los documentos a los que se refiere el escrito anterior:

1-Denuncia policial de *[dd/mm//aa]* (atestado n.º nnnn) y escrito de de *[dd/mm//aa]* del Director de los Servicios Generales del citado Hospital*[nombre del hospital]* relativa a los hechos que nos ocupan.
2- Comunicación a la ciudadanía de la existencia de una brecha de seguridad.
3- Información sobre la formación de profesionales y otros recursos.

Tercero. Propuesta de resolución. (art. 89 LPAC).

1.Finalizada la instrucción del procedimiento, se procedió a realizar la correspondiente propuesta de resolución, estableciendo el plazo de diez días para la formulación de alegaciones, de conformidad con el artículo 89.2 LPACAP y en relación con el artículo 73.1 de la misma norma.

2.Notificada la propuesta de resolución al órgano incoado el 10/06/2024, éste no presentó alegaciones.

HECHOS PROBADOS

De los documentos obrantes en el expediente y de las actuaciones practicadas, pueden considerarse como hechos probados:

Único. Se ha producido una brecha de seguridad con fecha 30 de mayo de 2023 en el Hospital *[nombre del hospital]* al haberse comprobado la pérdida de un disco duro externo del Servicio de Admisión y Documentación Clínica del citado centro hospitalario, conteniendo información del "Conjunto Mínimo Básico de Datos (CMBD)" de los últimos nnn años. El dispositivo no se encontraba cifrado, si bien quedaba custodiado en un armario con llave, la cual estaba en *[lugar]*, que no disponía de videovigilancia que pudiera haber registrado lo sucedido.

FUNDAMENTOS JURÍDICOS

Primero. Sobre la competencia.

1. De conformidad con lo previsto en el artículo 57.1 y 64.2 LOPDGDD y el artículo 43.1 LTPA en relación con el artículo 3.1 LTPA corresponde a este Consejo como autoridad autonómica de protección de datos personales y dentro de su ámbito competencial, el ejercicio de la potestad sancionadora y de los poderes previstos en el artículo 58 RGPD.

2. La competencia para la adopción de esta resolución reside en el Director, conforme al art. 48.1.i) LTPA y el art. 10.3.i) Estatutos.

3. Debe destacarse a su vez que, en virtud del artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, *"[e]l personal funcionario del Consejo, cuando realice funciones de investigación en materias propias de la competencia del Consejo, tendrá el carácter de agente de la autoridad"*, con las consecuencias que de aquí se derivan para los sujetos obligados en relación con la puesta a disposición de la información que les sea requerida en el curso de tales funciones investigadoras.

4. Este procedimiento se inicia como consecuencia de una presunta vulneración de la normativa de protección de datos por parte de una entidad bajo el control del Consejo en lo que respecta al cumplimiento de dicha normativa. Por ello, en el presente caso, solo serán analizadas y valoradas aquellas cuestiones planteadas por el reclamante, en relación con la materia de protección de datos personales, que queden incluidas dentro de la esfera de responsabilidad de la mencionada entidad.

Segundo. Sobre el tratamiento de datos personales.

1. El Art. 2.1. RGPD dispone: *"[e]l presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*".

2. El Art. 4.1 RGPD define «dato personal» como *"[t]oda 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"*.

   Los datos personales a los que se refiere la denuncia son datos de categoría especial referidos a la salud.

3. De acuerdo con el Art. 4.2 RGPD, el tratamiento de datos personales es *"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".*

   En este caso, el tratamiento relacionado con la reclamación es el posible acceso no deseado a datos de categorías especiales en un número estimado entre 50.000 y 100.000 personas.

   En relación a las operaciones de tratamiento realizadas la entidad reclamada dispone de Registro de Actividades de Tratamiento, habiendo informado que aquellas operaciones se enmarcarían en la actividad de tratamiento "Historia de Salud del Sistema Sanitario Público de Andalucía".

4. Por último el Art. 4.7 RGPD considera responsable del tratamiento a aquella *"...autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento..."* Esta identificación del responsable de tratamiento debe entenderse completada por la concreción del

tercero realizada en el art. 4.10 RGPD, e incluir por tanto a las "*personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable…"*.

El responsable de los tratamientos es la Dirección General de Asistencia Sanitaria y Resultados en Salud del Servicio Andaluz de Salud.

Tercero. Sobre la calificación jurídica de los hechos.

1. Preceptos infringidos.
   El artículo 5.1.f) RGPD establece el principio de *"integridad y confidencialidad"*, por el cual los datos personales serán *"tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".*

   Debe entenderse que este deber de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Dicho deber supone una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento, siendo además complementario del deber de secreto profesional.

   El artículo 32 RGPD se refiere a la "seguridad del tratamiento", y en su apartado primero establece que:

   > *"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".*

1.1. Consideraciones jurídicas sobre la existencia de infracción.
   De la documentación obrante en el expediente se comprueba que el responsable del tratamiento pudo incumplir por las circunstancias expuestas anteriormente, el mencionado artículo 32.1 RGPD en relación con la falta de aplicación de medidas técnicas y organizativas apropiadas para evitar el posible acceso no autorizado a datos de categorías especiales de un número estimado entre nnn y nnn personas, al haberse producido la pérdida o robo del mencionado dispositivo sin medidas de seguridad.

   Asimismo, por los motivos expuestos y por el carácter muy grave de los perjuicios potenciales para los derechos y libertades de las personas interesadas en tal número y en un contexto de atención sanita-

ria, podría haberse producido una vulneración sustancial del principio de confidencialidad, regulado en el artículo 5.1.f) RGPD.

En este mismo sentido el considerando 83 del RGPD señala que:

> *"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".*

1.2. Valoración de las alegaciones al acuerdo de inicio, pruebas practicadas o medidas provisionales.

En primer lugar el órgano incoado viene a exponer las medidas de seguridad existentes, indicando, resumidamente, que el *disco duro se guardaba en una dependencia del Servicio de Documentación Clínica, donde la entrada está restringida a los profesionales que prestan servicios en el mismo, haciendo constar que dicho servicio permanece siempre cerrado, limitándose su acceso sólo a los profesionales que trabajan en el mismo. Además, dicho disco duro se encontraba depositado en el interior de un armario con llave, junto a otro material de trabajo, guardándose la llave en el cajón de una mesa del personal administrativo, accediéndose a él, previa petición de la llave por parte de los referidos profesionales de la Unidad que lo requirieran. Por otro lado, existe una cámara de seguridad a la entrada del Servicio, que sólo graba el acceso al mismo, mas no el interior, donde se desarrolla el trabajo habitual, al no estar permitido.*

En relación con los hechos expuestos señalar que la pérdida o robo del citado disco duro que ha originado la incoación del presente expediente sancionador, evidencia que tales medidas han resultado claramente inapropiadas por insuficientes para garantizar la seguridad de los datos personales custodiados ante riesgos como la pérdida o robo, tal y como se exige por la normativa vigente anteriormente citada.

En segundo lugar, el órgano incoado expone que "(...) *a principios de 2023, se envió a los Servicios Centrales el Conjunto Mínimo Básico de Datos (CMBD) completo del año 2022. Este archivo está en formato ACCESS conteniendo datos numéricos (como fecha de nacimiento, código postal, ...) y alfanuméricos (como NUHSA,· datos clínicos codificados con CIE-10, ...), en el que no se identifican con nombre y apellidos a los usuarios y es imposible relacionar los datos que allí aparecen con un nombre de usuario, para ello necesitarían otra base de datos y cruzar la información. "*

Por tanto, el órgano incoado reconoce que el citado disco duro contenía datos personales (como fecha de nacimiento, código postal,como NUHSA,· datos clínicos codificados con CIE-10, ...).

Al respecto se indica que el RGPD dispone en su artículo 4.1 que se entiende por datos personales:

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

Y en su apartado 5, referente a la seudonimización , se indica:

"5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;"
(38) Por lo que respecta al carácter «identificable» de una persona, de la redacción del artículo 4, punto 1, del RGPD se desprende que una persona identificable es aquella que puede ser identificada no solo directa, sino también indirectamente.

El hecho de que el disco duro no contuviera los nombres y apellidos de los usuarios hace que se aprecie un cierto tratamiento de seudonimización que, en el mejor de los casos, podría evitar la identificación directa de los pacientes concretos pero no hace imposible ni descartable la determinación de dicha identidad de forma indirecta, máxime conteniendo el citado disco el NUHSA (Número de Historia Única de Salud de Andalucía) que es único e individual para cada persona, y de que dichos datos no se encontraban cifrados, tal y como se advierte en el formulario por el que se notifica a este Consejo laa violación de seguridad de datos personales utilizado por el órgano incoado, donde se indica que *"El disco no implementaba cifrado de datos y los archivos en él ubicados tampoco".*

En relación a esto, debemos traer a colación la reciente Jurisprudencia del Tribunal de Justicia de la Unión Europea sobre la consideración de dato personal como información de una persona física identificada o identificable. Por todas, la STJUE de 7 de marzo de 2024 (Sala Cuarta), asunto C-604/22:

(39) Como ya ha declarado el Tribunal de Justicia, el uso por el legislador de la Unión del término «indirectamente» muestra que, para calificar una información de dato personal, no es necesario que dicha información permita, por sí sola, identificar al interesado (véase, por analogía, la sentencia de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 41). Al contrario, del artículo 4, punto 5, del RGPD, en relación con el considerando 26 de dicho Reglamento, se desprende que los datos personales que cabría atribuir a una persona física mediante la utilización de información adicional deben considerarse información sobre una persona física identificable (sentencia de 5 de diciembre de 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, apartado 58).

(40) Por otra parte, ese considerando 26 precisa que, para determinar si una persona es «identificable», deben tenerse en cuenta «todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física». Dicho tenor sugiere que, para que un dato pueda ser calificado de «dato personal», en

el sentido del artículo 4, punto 1, de dicho Reglamento, no es necesario que toda la información que permita identificar al interesado se encuentre en poder de una sola persona (véase, por analogía, la sentencia de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 43).
[…]

(43) Pues bien, aun cuando una TC String no contiene en sí misma elementos que permitan la identificación directa del interesado, no es menos cierto, en primer lugar, que contiene las preferencias individuales de un usuario específico por lo que respecta a su consentimiento en el tratamiento de los datos personales que le conciernen, lo que constituye información «sobre una persona física», en el sentido del artículo 4, punto 1, del RGPD.

(44) En segundo lugar, también consta que, cuando la información contenida en una TC String se asocia con un identificador, como, en particular, la dirección IP del dispositivo de tal usuario, puede permitir crear un perfil de dicho usuario e identificar efectivamente a la persona a que se refiere específicamente tal información.

(45) En la medida en que el hecho de asociar una cadena compuesta por una combinación de letras y caracteres, como la TC String, con datos adicionales, en particular con la dirección IP del dispositivo de un usuario o con otros identificadores, permite identificar a dicho usuario, procede considerar que la TC String contiene información sobre un usuario identificable, por lo que constituye un dato personal, en el sentido del artículo 4, punto 1, del RGPD, lo que viene corroborado por el considerando 30 del RGPD, que se refiere expresamente a este supuesto.

(46) Esta interpretación no queda desvirtuada por el mero hecho de que la propia IAB Europe no pueda combinar la TC String con la dirección IP del dispositivo de un usuario y no tenga la posibilidad de acceder directamente a los datos tratados por sus miembros en el marco del TCF."

Por otro lado, de conformidad con la Disposición Adicional Primera de la LOPDGDD:

"2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado"

Téngase en cuenta al respecto que en el Anexo II el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad se prevé para la protección de los soportes de información la aplicación de la medida de criptografía en el nivel medio y alto, como es el caso. Concretamente:

"*5.5.2 Criptografía [mp.si.2]*
(…)Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, pendrives, memorias USB u otros de naturaleza análoga.
Requisitos.
– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

– *[mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.”*.

La asunción de los riesgos de un almacenamiento en un disco duro no cifrado, aún cuando el soporte de la información se encontrara en el interior de un armario, fue totalmente innecesaria pues, de la documentación obrante en el expediente se deduce que el SAS ofrece y ofrecía en el momento de producirse los hechos, servicios propios de almacenamiento de información en línea que eran una opción mucho más segura y operativa. Por consiguiente, no debió optarse por un medio de almacenamiento que era menos seguro y menos operativo, teniendo en cuenta además que el disco duro contenía datos de salud de un número tan elevado de interesados [entre nnn y nnn personas afectadas].

En cuanto a las medidas recomendadas e implementadas, así como las adoptadas, se trata de las siguientes:

“(…)
1. Comunicación vía administrativa a Ayuda Digital (*[dd/mm//aa]*).
2. Adoptar las medidas aconsejadas por Subdirección Provincial de Tecnologías de la Información y Comunicación, por el Responsable de Seguridad de la Información del Hospital *[nombre del hospital]*, y por las de "Ayuda Digital" desde la fecha de su recomendación :
- Ubicar los datos que manejamos sólo en un entorno seguro como es nnn.
- No utilizar el disco duro para copias de datos de usuarios ni cualquier información de carácter personal.
3. Formular denuncia en la Comisaría de Policía por la sustracción del disco duro, presentándose la misma con fecha *[dd/mm//aa]*.
4. Comunicación a la ciudadanía en la web del centro (Anexo 2)”.(…)”.

Por otra parte y en este sentido, en el propio texto de Comunicación a la Ciudadanía aportado por el órgano incoado se indica (el subrayado es nuestro):

“ (…) Notificamos a la ciudadanía la detección de una brecha de seguridad de datos a raíz de la reciente desaparición de un disco duro portátil que contenía copias de seguridad de CMDB (Conjunto Mínimo Básico de Datos) del Hospital *[nombre del hospital]* pudiendo afectar a la confidencialidad de los datos pero no a su disponibilidad ni a su integridad, que se mantienen en el sistema de almacenamiento principal del hospital. Se trata de un registro administrativo que contiene variables clínicas, demográficas y administrativas del proceso asistencial de los usuarios y las usuarias pero no incluye nombre, direcciones, teléfonos ni otros datos personales que permitan su identificación directa al estar codificada.(…). No esperamos ninguna consecuencia pero le recomendamos que esté atento a cualquier actividad anormal”.

Este Consejo valora muy positivamente la gestión realizada de la brecha de seguridad, incluyendo su comunicación a la ciudadanía, a las Fuerzas y cuerpos de seguridad y a este mismo Consejo.

Estas actuaciones sin embargo no eximen de la responsabilidad de la infracción por parte del responsable del tratamiento, que es previa a la comunicación de la brecha y del inicio del procedimiento sancionador.

De acuerdo con todo lo expuesto, entendemos que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

1.3. Tipificación.

Los hechos atribuidos al órgano incoado, por las razones expuestas, suponen las siguientes infracciones a la normativa de protección de datos personales:

El incumplimiento de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* del RGPD se contempla como infracción a la normativa de protección de datos personales en el artículo 83.5.a) RGPD; la mencionada conducta está igualmente tipificada como infracción muy grave en el artículo 72.1 a) LOPDGDD:

"El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".

El incumplimiento de *"las obligaciones del responsable y del encargado a tenor de los artículos 8,11, 25 a 39, 42 y 43"* del RGPD se contempla como infracción a la normativa de protección de datos personales en el artículo 83.4.a) RGPD; los hechos atribuibles al órgano imputado están igualmente tipificados como infracción grave en el artículo 73 f) LOPDGDD:

"La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".

Cuarto. Sobre la identificación de la entidad responsable (art. 89.3 LPAC).

De conformidad con lo previsto en el artículo 70.1 LOPDGDD, se identifica como entidad responsable de la infracción, a la Dirección General de Asistencia Sanitaria y Resultados en Salud (Servicio Andaluz de Salud).

Quinto. Declaración de la infracción y medidas a adoptar (art. 77.2 LPAC y 58.2 RGPD).

1. El artículo 77 LOPDGDD establece el régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento; incluyendo, entre otros a:

> *"a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
> *[...]*
> *c) [...] las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
> *e) Las autoridades administrativas independientes.*
> *[...]*

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de [...] las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

En el mencionado artículo, en su apartado 2, se señala que:

"Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.[...]".

A su vez, en su apartado 3, se señala que:

"Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda."

Así, de acuerdo con el artículo 77.2 LOPDGDD, procede declarar la infracción o infracciones antes descritas.

2. Por otra parte, en relación con las medidas que proceda adoptar, el artículo 58.2 RGPD dispone que:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: [...]

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

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición; [...]

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional. [...]".

Respecto a las posibles medidas que proceda adoptar, no se considera preciso ordenar al órgano incoado la puesta en marcha de medidas adicionales a las ya adoptadas.

Sexto. Notificaciones y comunicaciones.
En relación con la notificación de la resolución del procedimiento sancionador, el artículo 77.2 LOPDGDD dispone que "*[l]a resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso*".

Además, el artículo 77.4 LOPDGDD señala que "*[s]e deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores*", y el 77.56 LOPDGDD, que "*[s]e comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo*".

En virtud de todo lo expuesto, el director del Consejo de Transparencia y Protección de Datos de Andalucía dicta la siguiente,

RESOLUCIÓN

Primero. Declarar la infracción responsabilidad de la Dirección General de Asistencia Sanitaria y Resultados en Salud (Servicio Andaluz de Salud, con NIF *[NNNNN]*), por la comisión de las siguientes infracciones:

El incumplimiento de *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* del RGPD se contempla como infracción a la normativa de protección de datos personales en el artículo 83.5.a) RGPD; la mencionada conducta está igualmente tipificada como infracción muy grave en el artículo 72.1 a) LOPDGDD:

"El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".

El incumplimiento de *"las obligaciones del responsable y del encargado a tenor de los artículos 8,11, 25 a 39, 42 y 43"* del RGPD se contempla como infracción a la normativa de protección de datos personales en el artículo 83.4.a) RGPD; los hechos atribuibles al órgano imputado están igualmente tipificados como infracción grave en el artículo 73 f) LOPDGDD:

"La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".

Segundo. Respecto a las posibles medidas que proceda adoptar, no se considera preciso ordenar al órgano incoado la puesta en marcha de medidas adicionales a las ya adoptadas.

Tercero. Que, una vez dictada, se notifique la resolución al órgano infractor y a la Dirección Gerencia del Servicio Andaluz de Salud.

Cuarto. Que se comunique la presente resolución al Defensor del Pueblo Andaluz, de conformidad con lo establecido en el artículo 77.5 LOPDGDD

En consonancia con lo establecido en el artículo 50 LOPDGDD, la presente Resolución se hará pública, disociando los datos que corresponda, una vez haya sido notificada a los interesados.

El incumplimiento de esta resolución podría comportar la comisión de la infracción considerada en el artículo 72.1.m) LOPDGDD, sancionable de acuerdo con el artículo 58.2 RGPD.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer recurso potestativo de reposición ante este Consejo, en el plazo de un mes, o interponer directamente recurso contencioso-administrativo ante el Juzgado de lo Contencioso Administrativo de Sevilla que por turno corresponda, en el plazo de dos meses, en ambos casos a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 30.4, 123 y 124 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en los artículos 8.3 y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

No obstante, al tratarse de un acto en materia de sanciones, el demandante podrá elegir alternativamente interponer el citado recurso contencioso-administrativo ante el juzgado o el tribunal en cuya circunscripción tenga aquél su domicilio, siempre entendiendo esta elección limitada a la circunscripción del Tribunal Superior de Justicia de Andalucía, de conformidad con lo dispuesto en los apartados segundo y tercero del artículo 14.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Conforme a lo previsto en el art. 90.3.a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta ante este Consejo su intención de interponer recurso contencioso-administrativo y traslada al mismo, una vez interpuesto, la documentación que acredite su presentación. Si el Consejo no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo correspondiente o en dicho recurso no se solicitara la suspensión cautelar de la resolución, se daría por finalizada la mencionada suspensión.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López