

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 56/2021, referente a la Fundación San Francisco de Asís.

Antecedentes

1. Entre los meses de abril y mayo de 2021 tuvieron entrada en la Autoridad Catalana de Protección de Datos veinticuatro denuncias formuladas por distintas personas contra la Fundación San Francisco de Asís (en adelante, FSFA), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales. A estas denuncias se les asignó los núm. 133, 134, 135, 137, 138, 139, 140, 142, 143, 144, 145, 146, 147, 148, 149, 151, 156, 158, 168, 17

Las personas denunciantes -todas ellas empleadas de la FSFA- se quejaban de accesos no justificados a su historia clínica compartida (HC3) llevados a cabo por alguna persona o personas empleadas del Centro de (...), gestionado por la FSFA. Todas las personas denunciantes indicaban que estos accesos no estarían justificados en la medida en que no eran pacientes/usuarios de dicho centro.

Para acreditar los hechos denunciados, cada una de las personas denunciantes aportaba copia del registro de accesos a su HC3 -extraído del portal "Mi Salud" (en adelante, LMS) del Departamento de Salud- en el que figuraban los accesos efectuados desde el Centro (...). Todos los accesos que constaban en los listados de LMS aportados por las personas denunciantes se habían efectuado entre 2019 y 2020, con el detalle que se indicará en los hechos probados.

2. La Autoridad abrió una fase de información previa de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 11/06/2021 se dio traslado a la FSFA de un listado en el que constaban los accesos denunciados referidos a veinticuatro personas empleadas de su entidad, y se le requirió para que diera cumplimiento a lo siguiente:

- Aportara una copia del registro de accesos a cada una de las HC3 de las personas denunciantes, en la que constara los accesos realizados desde el Centro (...) de la FSFA entre 28/10/2019 y el 31/05/2021 .
- Informara si la FSFA, en las fechas en que se produjeron los accesos controvertidos, tenía implementadas en el sistema de gestión y consulta de historias clínicas, las medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluyera un proceso de verificación ,

evaluación y valoración regulares de la eficacia de las medidas de seguridad adoptadas, como podría ser la exigencia de efectuar una revisión mensual de la información registrada sobre los accesos al HC3 por parte del personal al servicio de la FSFA, con la elaboración del correspondiente informe.

4. En fecha 02/07/2021, la FSFA respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- En cuanto al registro de accesos al HC3 de cada una de las personas denunciadas, informaban que no disponían de dicho registro dado lo siguiente:

"Durante este período, la FSFA disponía de dos métodos de acceso al HC3:

- Desde la plataforma de compartición de los datos clínicos del Barcelonès Nord y el Maresme de Badalona Servicios Asistenciales BSA (esta plataforma forma parte del SIO de la red pública salud que no dispone de aplicaciones de gestión de historias clínicas que fueran compatibles). Desde el 03/11/2009 la FSFA está inscrita en el convenio tipo para implantar la Historia Clínica Compartida en Cataluña y el acceso se efectuaba tal y como se describe en el convenio, con certificado de dispositivo de aplicación (CDA) emitido por la Agencia Catalana de Certificación (CATCert) en BSA. Adjuntamos como Anexo 1 el convenio firmado y como Anexo 2 el formulario de incorporación. El acceso se llevaba a cabo a través del portal web de BSA, no disponiendo en nuestra organización de ningún registro de estos accesos.

- Desde el programa asistencial GENOMI. Desde el 18/10/2019 se podía acceder al HC3 desde dentro del Programa con conexión a través de URL Visor autorizada por el área de soporte HC3 del TICSalut del Departamento de Salud de la Generalitat. Todos los accesos realizados desde este método quedan registrados en el programa GENOMI, identificando el usuario que hace la consulta, la fecha y la hora en que se realizó, el CIP del paciente consultado y el identificador de la Historia Clínica (NHC) a la que se ha intentado acceder.

En el registro de accesos del programa asistencial GENOMI no aparece ninguno de los accesos referenciados en el anexo del requerimiento, por tanto los accesos objeto de denuncia sólo se han efectuado desde la plataforma de compartición de los datos clínicos del Barcelonès Nord y el Maresme de Badalona Servicios Asistenciales y por eso no podemos facilitar la información solicitada.

En la actualidad, el acceso a través de BSA está totalmente inutilizado e inoperativo".

- Sobre la identificación de la persona o personas que efectuaron el acceso, informan que:

"No tenemos registros para saber el usuario que ha realizado las consultas solicitadas, el acceso a la plataforma BSA requería de un usuario con contraseña y también tener el certificado digital instalado en el ordenador, en el que sólo hay tenían acceso las personas autorizadas por la FSFA, pertenecientes al servicio médico (médicos), rehabilitación, psicología y atención al usuario. Este certificado sólo estaba instalado en unos ordenadores concretos ubicados en nuestras instalaciones, y dentro de estos ordenadores sólo tenían acceso las personas autorizadas ya que sólo estaba habilitado en sus sesiones de usuario.

El resto de trabajadores no disponían de este certificado. Este certificado era el mismo para todos los usuarios, facilitado por BSA y estaba a nombre de "CSS (...)_(...)", por lo que no se puede identificar a la persona que ha realizado estas consultas.

Sólo podemos identificar los accesos realizados durante el año 2020, que han sido efectuados por el personal del centro (...), con conocimiento del (...). (...), (...), de la FSFA y realizados por los motivos y el contexto expuestos en el punto 1.b."

- Sobre la justificación de los accesos, se informaba de lo siguiente:

"No tenemos constancia del motivo de los accesos realizados durante los días 28/10/2019, 17/09/2020 y 01/12/2020 ya que no se ha podido identificar a la persona que los ha realizado para que nos los justifique.

Los accesos de los días 14/04, 21/04, 01/05, 17/09 y 01/12 del año 2020 se realizaron por seguimiento por contacto estrecho con casos posibles/probables o confirmados de COVID19, en el contexto de aumento de casos debidos a las diferentes oleadas de la pandemia, puesto que no teníamos información fiable del trabajador afectado en cada caso.

Del resto de accesos, efectuados en el mes de mayo de 2020 tienen que ver con la siguiente situación: en los meses de abril y mayo de 2020 el impacto de la primera ola de la pandemia de la COVID19 en las entidades como la nuestra era muy relevante (...).

Todos nuestros usuarios son personas muy frágiles y por tanto de alto riesgo frente a una posible infección por la COVID (...). En esas fechas la Organización no gubernamental OPEN ARMS contactó con nuestra entidad, y entre otras (...) se ofreció a realizar un cribado de PCR's a todos los usuarios y profesionales de nuestra entidad. Se hizo la recogida de muestras el día domingo diez de mayo de 2020, y fueron derivadas a dos laboratorios (...) La necesidad de conocer los resultados con la máxima urgencia, en el contexto de infecciones y defunciones antes citado y ante la emergencia de adoptar decisiones, ya sea en relación a usuarios o en relación a profesionales, para frenar la expansión de las infecciones, supuso que desde la Dirección General se valorara la necesidad de acceder al HC3, con la única finalidad de conocer los resultados de las PCR's analizadas (...) y así evitar el crecimiento de los contagios y muertes".

- Que "en las fechas solicitadas no se tenía ningún proceso de verificación de accesos implementado, ya que como se ha comentado anteriormente, no se podía controlar los accesos desde la plataforma de compartición de los datos clínicos del Barcelonès Nord y el Maresme de Badalona Servicios Asistenciales BSA (sólo limitar a los usuarios que tenían acceso que ya se hacía instalando sólo el certificado en las sesiones de usuario de las personas autorizadas, y otorgando un usuario y contraseña propio a cada uno).

Con la implementación del programa asistencial GENOMI sí que tenemos acceso al registro de todos los accesos que se realizan al HC3, pero hasta inicios de 2021, que se detectaron posibles accesos indebidos, no se han realizado valoraciones regulares del eficacia de las medidas de seguridad".

La entidad denunciada adjuntaba al escrito documentación diversa, entre otros:

- a) "Convenio tipo para implantar la Historia clínica compartida en Cataluña" de 9 de julio de 2009.

En el punto quinto de este convenio, referente al "Acceso a la HCCC en cada centro", figura el siguiente literal:

"1. De acuerdo con lo que se establece en la normativa sanitaria y de protección de datos, únicamente las personas autorizadas pueden tener acceso a la información contenida en la HCC.

La entidad que suscribe este convenio se obliga a facilitar los sistemas de identificación y autenticación individualizados de sus profesionales sanitarios que, de acuerdo con los puntos tercero y cuarto de este pacto, puedan acceder a la HCCC (...).

2. (...) Este centro es responsable de informar a los miembros de su personal autorizado con acceso autorizado que cada uno asume la responsabilidad de proteger los datos o los sistemas de identificación y autenticación y que su uso implica la aceptación y el conocimiento de derechos y deberes en relación con el acceso al HCCC".

Y en el anexo 6, apartado A de este convenio, en lo referente a las "medidas estándar aplicadas" se recoge lo siguiente:

"De la misma manera que se requiere protección lógica del acceso a los datos, también se requiere una protección física, es decir, sólo los profesionales autorizados deben tener acceso a los datos clínicos".

b) "Programa de Historia Clínica Compartida en Cataluña (HCCC). Especificaciones para la conexión de los centros al sistema.

En el apartado 4.4, en lo referente al "Certificado CATCert", se indica que "El servidor web debe contar con un certificado emitido por el CATCert. Lo utilizará para demostrar su identidad en la comunicación SSL con el HCCCSs de la plataforma central"

c) "Programa de Historia clínica compartida en Cataluña (HCCC). Formulario de incorporación", formalizado entre el Departamento de Salud y la FSFA el 3/11/2009.

En este documento se indica que se incorpora al programa de HC3 el Centro Sociosanitario (...), y que "Para el acceso a los servicios que presta el HCCC, se utilizarán certificados de dispositivo de aplicación (CDA) emitidos por la Agencia Catalana de Certificación - CATCert con los siguientes datos de identificación: Organización. BSA".

d) "Informe registro accesos HC3 núm. RI-2021-001" emitido por la FSFA el 12/03/2021, en el que hay una anotación el día 17/02/2021 con el siguiente literal: *El Responsable TI bloquea CONEXIONES HCCC on existe el certificado original, la contraseña para instalarlo y las credenciales para acceder al HC3 a través del BSA".*

e) "Protocolo acceso historia clínica compartida en Cataluña (HC3) – Documento de Seguridad FSFA" elaborado por el delegado de protección de datos de la FSFA en febrero de 2021. En este documento, entre otras cuestiones, se definen las condiciones para acceder al HC3; y en éste

sentido se determina que *“para accederse necesita un usuario y contraseña unipersonales que sólo se facilitarán a los usuarios descritos en el apartado “Responsables autorizados con acceso al HC3”; los usuarios creados y la persona a la que se le asigna quedan anotados en el anexo del Documento de Seguridad: DS_Anexo_17.1 Usuarios Acces HC3 y SIRE.”*

5. En fecha 08/07/2021 se requirió al Departamento de Salud, como responsable del fichero de HC3, que aportara una copia del registro de accesos al HC3 de cada una de las personas denunciantes (qué listado se adjuntaba al oficio), desde el 28/10/2019 hasta el 31/05/2021, y que incluyera aquellos accesos efectuados desde el Centro Sociosanitario (...), dependiente de la FSFA.

6. En fechas 22/07/2021 y 30/07/2021 el Departamento de Salud dio cumplimiento a este requerimiento aportando una copia de los registro de accesos a las HC3 de las personas denunciantes en el período indicado. En estos registros se observa que todos los accesos a dichas historias se habían efectuado con (...)(...)“(...).”

7. En fecha 05/10/2021 y aún en el marco de esta fase de información previa, se dio traslado a la FSFA de los registros de accesos a las HC3 de los denunciantes que el Departamento de Salud había proporcionado a la misma Autoridad, y en relación con el que se le requirió la siguiente información:

- Que, a la vista de los registros proporcionados por el Departamento de Salud en el que constan que todos los accesos a las HC3 de los denunciantes fueran realizados por el (...), cumplimentara, en su caso, la información proporcionada a esta Autoridad en el escrito de 02/07/2021, en relación con la justificación de los accesos.
- Que informara si la FSFA disponía de un único usuario/contraseña para acceder a la plataforma BSA para consultar el registro del HC3; o bien, si cada persona con acceso a dicha plataforma disponía de un usuario/contraseña personal.

8. En fecha 15/10/2021, la FSFA dio cumplimiento a este requerimiento mediante escrito a través del cual manifestaba lo siguiente:

- Que, en relación con la justificación de los accesos, no pueden facilitar más información que esa que ya se proporcionó.
- Que la plataforma de compartición de los datos clínicos del Barcelonès Nord y el Maresme de Badalona Servicios Asistenciales yBSA” *“fue creada el Servicio Catalán de la Salud y permitía el acceso al HC3 a aquellos proveedores de la red pública de salud que no disponían de aplicaciones de gestión de historias clínicas que fueran compatibles, aplicación que no gestionábamos directamente desde la Fundación”*.
- Que *“el acceso a la plataforma BSA requería de un usuario con contraseña y también tener el certificado digital instalado en el ordenador, al que sólo tenían acceso las personas autorizadas por la FSFA. La Fundación sólo tenía un solo usuario para todo el personal autorizado para acceder a la plataforma BSA”*.

9. En fecha 30/11/2021, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra la FSFA por tres presuntas infracciones: una infracción prevista en el artículo 83.5.a) en relación con el artículo 5.f); y dos infracciones previstas en el artículo 83.4.a) en relación con el artículo 32; todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 30/11/2021.

10. En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

11. En fecha 13/12/2021 la FSFA solicitó la ampliación del plazo para formular alegaciones, el cual le fue concedido mediante acuerdo de la instructora del procedimiento de fecha 14/12/2021, notificado aquél mismo día.

12. En fecha 22/12/2021 tuvo entrada un escrito de la FSFA en el que no cuestionaba los hechos imputados al procedimiento ni tampoco su calificación jurídica, al contrario, reconocía su responsabilidad. En el mismo escrito la entidad reiteraba lo expuesto en el marco de la información previa en relación con las circunstancias que habían propiciado los accesos a las historias clínicas de sus trabajadores llevados a cabo entre los meses de abril y mayo de 2020 ; y, detallaba las medidas que se habían tomado para evitar que en un futuro pudieran producirse hechos como los que habían dado lugar al presente procedimiento sancionador. Por último, el FAMT enunciaba aquellas circunstancias atenuantes que a su juicio concurrían en el presente caso para que se tuvieran en cuenta a la hora de establecer la cuantía de la sanción.

13. En fecha 01/03/2022, la instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos impusiera a la FSFA dos sanciones consistentes en dos multas administrativas, una de 8.000 euros (ocho mil euros), como responsable de una infracción prevista en el artículo 85.5.a), en relación con el artículo 5.1.a); y, una multa de 2.000 euros (dos mil euros) por la infracción prevista en el artículo 85.4.a), en relación con el artículo 32, todos ellos del RGPD.

Esta propuesta de resolución se notificó en fecha 02/03/2022 y se concedía un plazo de 10 días para formular alegaciones.

14. El plazo se ha superado con creces y no se han presentado alegaciones a la propuesta de resolución.

15. En fecha 04/03/2022, la entidad imputada pagó por adelantado 6.000 euros (seis mil euros), correspondientes a la suma de las sanciones pecuniarias propuestas por la instructora en la propuesta de resolución, una vez aplicadas las reducciones previstas en el artículo 85 de la ley

39/2015. En este punto cabe recordar que en el escrito de 22/12/2021 (antecedente 12) la entidad reconoció su responsabilidad en los hechos imputados.

Hechos probados

1. Mediante el certificado digital vinculado al (...). (...) -que le permitía el acceso al fichero de HC3 del Departamento de Salud a través de la plataforma BSA- una persona o personas no identificadas accedieron a las HC3 de las personas denunciadas -todas ellas trabajadoras de la entidad-, sin que los accesos estuvieran justificados por una razón asistencial o administrativa. La relación de accesos indebidos son los siguientes:

TITULAR HC3	Fecha y hora del acceso	Información Consultada
(133) (...)	28-10-2019 12:06	Información historia clínica resumen
	28-10-2019 12:08	Información Curso clínico Integrado
	28-10-2019 12:11	Información informes clínicos
(134) (...)	28-10-2019 12:16	Información historia clínica resumen
	28-10-2019 12:17	Información curso clínico Integrado
	28-10-2019 12:19	Información informes clínicos
	28-10-2019 12:19	Información historia clínica resumen
	15-05-2020 09:12	Información historia clínica resumen
(135) (...)	15-05-2020 09:12	Información historia clínica resumen
(137) (...)	15-05-2020 10:16	Información historia clínica resumen
(138) (...)	14-05-2020 18:27	Información historia clínica resumen
	15-05-2020 09:03	Información historia clínica resumen
(139) (...)	14-04-2020 18:14	Información historia clínica resumen
	14-04-2020 18:16	Información informes clínicos
	14-04-2020 18:19	Información historia clínica resumen
	14-04-2020 18:19	Información informes clínicos
	15-05-2020 08:43	Información historia clínica resumen
(140) (...)	28-10-2019 12:27	Información Curso clínico Integrado
	28-10-2019 12:27	Información historia clínica resumen
	28-10-2019 12:29	Información historia clínica resumen
	15-05-2020 09:48	Información historia clínica resumen
(142) (...)	15-05-2020 10:25	Información historia clínica resumen
(143) (...)	15-05-2020 09:30	Información historia clínica resumen
(144) (...)	28-10-2019 12:13	Información informes clínicos
	28-10-2019 12:13	Información historia clínica resumen
	28-10-2019 12:14	Información Curso clínico Integrado
	15-05-2020 08:38	Información historia clínica resumen
	15-05-2020 08:41	Información historia clínica resumen
	15-05-2020 09:51	Información historia clínica resumen

(145) (...)	15-05-2020 08:59	Información historia clínica resumen
(146) (...)	28/10/2019 12:24	Información historia clínica resumen
	28/10/2019 12:24	Información Curso clínico Integrado
	28/10/2019 12:24	Información Curso clínico Integrado
	15/05/2020 09:27	Información historia clínica resumen
	18/05/2020 17:19	Información historia clínica resumen
	18/05/2020 17:21	Información historia clínica resumen
(147) (...)	15-05-2020 10:44	Información historia clínica resumen
	01-12-2020 15:10	Información historia clínica resumen
(148) (...)	15-05-2020 10:23	Información historia clínica resumen
	15-05-2020 11:50	Información historia clínica resumen
(149) (...)	15-05-2020 09:06	Información historia clínica resumen
(151) (...)	15-05-2020 08:48	Información historia clínica resumen
(156) (...)	01-05-2020 11:00	Información historia clínica resumen
	15-05-2020 08:56	Información historia clínica resumen
(158) (...)	15-05-2020 09:52	Información historia clínica resumen
	20-05-2020 13:12	Información historia clínica resumen
	17-09-2020 07:41	Información historia clínica resumen
(165) (...)	15-05-2020 08:52	Información historia clínica resumen
(170) (...)	14-04-2020 18:20	Información historia clínica resumen
	14-04-2020 18:20	Información informes clínicos
	21-04-2020 14:14	Información historia clínica resumen
	21-04-2020 14:14	Información Curso Clínico integrado
	15-05-2020 16:46	Información historia clínica resumen
(186) (...)	15-05-2020 10:00	Información historia clínica resumen
(187) (...)	28-10-2019 12:20	Información historia clínica resumen
	28-10-2019 12:21	Información Curso Clínico integrado
	28-10-2019 12:22	Información informes clínicos
	15-05-2020 09:46	Información historia clínica resumen
(188) (...)	14-04-2020 18:33	Información historia clínica resumen
	14-04-2020 18:33	Información informes clínicos
	15-05-2020 10:16	Información historia clínica resumen
(202) (...)	15-05-2020 09:14	Información historia clínica resumen

2. El certificado digital vinculado al (...). (...) de la FSFA -que como se ha dicho en el punto precedente, permitía el acceso al fichero de HC3 mediante la plataforma BSA- fue instalado en varios ordenadores a los que tenían acceso distintas personas también trabajadoras de la entidad. Así, en la medida en que

todas estas personas podían utilizar el mismo certificado para acceder a la base de datos de HC3, no se podía garantizar la identificación de forma inequívoca y personalizada de la persona que efectivamente accedía, ni en consecuencia, tampoco analizar la justificación de éstos accesos.

Esta situación se habría mantenido al menos hasta el 17/02/2021, fecha en la que, según el informe elaborado por la FSFA y aportado a esta Autoridad, el acceso a la base de datos del HC3 a través de la plataforma BSA se bloqueó (letra de antecedente 4º).

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC, y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2ª de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos. Los hechos objeto de este procedimiento recaen en el ámbito competencial de la Autoridad en virtud del artículo 3.f) de la Ley 32/2010.

2. De conformidad con el artículo 85.3 de la LPAC, tanto el reconocimiento de responsabilidad como el pago voluntario adelantado de la sanción pecuniaria propuesta comportan la aplicación de unas reducciones. La efectividad de estas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por vía administrativa contra la sanción. Para ambos casos, los apartados 1 y 2 del artículo 85 de la LPAC contemplan la terminación del procedimiento.

La entidad imputada no formuló alegaciones al acuerdo de iniciación y tampoco lo hizo ante la propuesta de resolución, acogándose a ambas opciones para reducir el importe de la sanción. Sin embargo, se considera oportuno reiterar las apreciaciones hechas por la instructora sobre las circunstancias que, según la FSFA, habrían propiciado los accesos que se produjeron entre los meses de abril y mayo de 2020 en las historias clínicas de las personas denunciadas (antecedente 4º), en esencia, la necesidad de conocer lo antes posible el resultado de las pruebas PCR a las que se habían sometido las personas trabajadoras del centro, a la vista de la vulnerabilidad de sus usuarios.

Al respecto, cabe decir que esta Autoridad es totalmente conocedora de la altísima presión asistencial que sufrieron los centros sanitarios y sociosanitarios en las fechas en que se produjeron muchos de los accesos que se consideran ilícitos (abril-mayo de 2020); pero esta situación excepcional no puede amparar en modo alguno la vulneración de la normativa de protección de datos, en este caso, el acceso a los historiales clínicos de las personas trabajadoras, historiales que por supuesto incluyen información que no se limita al resultado de determinadas pruebas, sino que abarca mucha más información clínica, que es susceptible de ser conocida por la persona que accede de acuerdo a su perfil. Como añadidura, también hay que poner de relieve que no sólo hay

había accesos a determinadas historias clínicas en 2020, es decir, en situación de pandemia, sino también en 2019, previos, pues, a esta situación.

3. En relación con el hecho descrito en el apartado 1 de hechos probados, relativo al principio de licitud, se debe acudir al artículo 6 del RGPD, que prevé 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 se parte o para la aplicación a petición del mismo 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 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.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de modo más preciso requisitos específicos de tratamiento y otras medidas que garantizan un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento (...).”

Por su parte, el artículo 9 del RGPD, relativo al tratamiento de categorías especiales de datos - cómo serían los datos de salud-, determina lo siguiente:

“1. Quedan prohibidos el tratamiento de datos personales que revelan el origen étnico o 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 forma unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual u orientaciones sexuales 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 dichas 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 de los Estados miembros o un convenio colectivo conforme 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 oa personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comunican 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, en base al 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, en base al 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, en base al 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.

3. Las datos personales a que se refiere el apartado 1 podrán tratarse en los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Y el artículo 9 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), referido a las categorías especiales de datos, entre las que se encuentran los datos de salud, determina en su apartado 2 lo siguiente:

2. Los tratamientos de datos previstos en las letras g), h) y i) del artículo 9.2 del Reglamento (UE) 2016/679 fundamentados en el derecho español estarán amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, esta norma puede amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y los servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

La legislación sanitaria, aplicable al caso, regula el uso de la historia clínica en los siguientes términos:

- Artículo 11 Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica:

Usos de la historia clínica

1. *La historia clínica es un instrumento destinado fundamentalmente a ayudar a garantizar una asistencia adecuada al paciente. A tal efecto, los profesionales asistenciales del centro que están implicados en el diagnóstico o tratamiento del enfermo deben tener acceso a la historia clínica.*

2. *Cada centro debe establecer el mecanismo que haga posible que, mientras se presta asistencia a un paciente concreto, los profesionales que lo atienden puedan, en todo momento, tener acceso a la historia clínica correspondiente.*

3. *Se puede acceder a la historia clínica con fines epidemiológicos, de investigación o docencia, con sujeción a lo que establece la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y la Ley del Estado 14/1986, de 25 de abril, general de sanidad, y las disposiciones concordantes. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, salvo que éste haya dado antes su consentimiento.*

4. *El personal que cuida de las tareas de administración y gestión de los centros sanitarios puede acceder sólo a los datos de la historia clínica relacionados con dichas funciones.*

5. *El personal al servicio de la Administración sanitaria que ejerce funciones de inspección, debidamente acreditado, puede acceder a las historias clínicas, a fin de comprobar la calidad de la asistencia, el cumplimiento de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes o la administración sanitaria.*

6. *Todo el personal que accede en uso de sus competencias a cualquier clase de datos de la historia clínica queda sujeto al deber de guardar su secreto.*

- Artículo 16 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":

"Artículo 16. Usos de la historia clínica.

1. *La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica del mismo como instrumento fundamental para su adecuada asistencia.*

2. *Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.*

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se regirá por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de modo que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Asimismo, se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los que se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso deberá realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración de que solicitara el acceso a los datos.

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionadas con sus propias funciones.

5. 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.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso”.

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el punto 1 del apartado de hechos probados, que se considera constitutivo de la infracción prevista en el artículo 83.5.a) del RGPD, que tipifica como tal la vulneración de “los principios básicos para el tratamiento”, entre los que se da lugar el principio de licitud.

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

La conducta que aquí se aborda se ha recogido como infracción muy grave en el artículo 72.1.e) de la LOPDDDD, en la siguiente forma:

“El tratamiento de datos personales de las categorías a que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que se dé alguna de las circunstancias previstas en el citado precepto y el artículo 9 de esta Ley orgánica”

4. Con respecto al hecho descrito en el punto 2 del apartado de hechos probados, relativo a la seguridad de los datos, se debe acudir al artículo 32 del RGPD, el cual dispone que:

“1. Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las 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 de los datos, el tipo y el alcance de los sistemas de información física o técnica; c) la capacidad de restaurar la disponibilidad y el acceso a los datos.”

la capacidad de restaurar la disponibilidad y el acceso a los datos

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. 3.

La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo. 4.

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

También el artículo 9.4 de la ya citada Ley 21/2000, determina que “los centros sanitarios deben tomar las medidas técnicas y organizativas adecuadas para proteger los datos personales

recogidas y evitar su destrucción o pérdida accidental, así como el acceso, alteración, comunicación o cualquier otro procesamiento que no sean autorizados”.

Respecto a la conducta descrita en el punto 2 del apartado de hechos probados, se considera que la FSFA ha vulnerado la seguridad de los datos ya que, por un lado, las credenciales vinculadas a un trabajador de la entidad, que permitían el acceso al HC3 a través de la plataforma BSA, fueron utilizadas indistintamente por otras personas trabajadoras de la organización, por lo que resultaba imposible identificar qué persona concreta habría realizado determinados accesos o actividades en relación con las HC3. Y por otra parte, la utilización de las mismas credenciales por distintas personas habría propiciado, a su vez, que la FSFA no pudiera analizar la justificación de los accesos al HC3 realizados por su personal.

De conformidad con lo expuesto, la conducta descrita en el punto 2 del apartado de hechos probados constituye una infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de “*las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43*”, entre las que se encuentra la obligación descrita en el artículo 32 referida a la seguridad del tratamiento.

A su vez, esta conducta se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679"

5. Al no albergarse la FSFA en ninguno de los sujetos previstos en el artículo 77.1 del LODGDD, resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD.

El artículo 83 del RGPD prevé para las infracciones previstas en su apartado 4, se sancionen con una multa administrativa de 10.000.000 de euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Por su parte, el apartado 5 del mismo precepto contemplado por las infracciones allí previstas se sancionen con multas administrativas de 20.000 euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Esto, sin perjuicio de que, con carácter adicional o sustitutivo, se puedan aplicar las medidas previstas en las dicciones a) ah) yj) del artículo 58.2 RGPD.

En el presente caso, tal y como exponía la instructora en la propuesta de resolución, procede descartar la posibilidad de sustituir la sanción de multa administrativa por la sanción de amonestación prevista en el artículo 58.2.b) RGPD, dado que las infracciones imputadas están vinculadas a tratamientos de datos de salud (que forman parte de las llamadas categorías especiales de datos).

Descartado que proceda sustituir la sanción de multa administrativa por una amonestación, corresponde determinar la cuantía de las sanciones de multa administrativa que corresponde imponer. Según lo que establece el artículo 83.2 del RGPD, y también de conformidad con el principio de proporcionalidad consagrado al artículo 29 de la Ley 40/2015, tal y como indicaba la instructora en la propuesta de resolución, procede imponer las sanciones de multas administrativas que se indican a continuación en base a la ponderación entre los criterios agravantes y atenuantes que se detallan:

5.1. Por lo que se refiere al hecho probado 1, relativo al principio de licitud, 8.000 euros (ocho mil euros).

5.2. Por lo que se refiere al hecho probado 2, relativo a la vulneración de la seguridad de los datos: 2.000 euros (dos mil euros).

La cuantificación de las multas se basa en la ponderación entre los criterios agravantes y atenuantes que se indican a continuación:

Por un lado, se aprecian las siguientes circunstancias que operan como criterios atenuantes en la graduación de las multas vinculadas a los dos hechos probados:

- La adhesión por parte de la FSFA al código de conducta de la Unión Catalana de Hospitales (art. 83.2.j RGPD).
- La falta de beneficios obtenidos como consecuencia de la comisión de la infracción (art. 83.2.k RGPD y art. 76.2.c LOPDGDD).
- Que la FSFA es una entidad sin ánimo de lucro (art. 83.2.k).

Aparte de estos atenuantes que, como se ha dicho, se han tenido en cuenta en la graduación de las dos multas que se proponen imponer, es necesario tener en consideración el siguiente criterio atenuante vinculado al hecho probado 1º.

- Falta de intencionalidad (art. 83.2.b RGPD).

Y, el siguiente atenuante vinculado al hecho probado 2º:

- Según consta en las actuaciones, FSFA había bloqueado el acceso al HC3 a través de la plataforma del BSA antes de que tuviera conocimiento del inicio de actuaciones inspectoras por parte de esta Autoridad (art. 83.2.k RGPD).

Por lo que se refiere al análisis de las circunstancias atenuantes que se han relacionado y que se han tenido en consideración a la hora de fijar la cuantía de las sanciones de multa, cabe señalar que la mayor parte de ellas han sido invocadas por la FSFA. Por el contrario, esta Autoridad no puede tener en cuenta como circunstancia atenuante -invocada por la entidad- la situación excepcional de pandemia que se dio a partir de marzo de 2020 y que habría llevado a acceder a las historias clínicas de sus trabajadores. Como ya se ha avanzado en el fundamento de derecho 2º, la situación complicada y ciertamente

excepcional que se dio en aquellos momentos en los centros sociosanitarios no podía amparar en modo alguno el acceso a las historias clínicas de las personas afectadas. Aparte de que, como también se ha dicho, algunos de los accesos fueron anteriores a dicho período.

En contraposición a las causas atenuantes expuestas, concurren sin embargo una serie de criterios del artículo 83.2 del RGPD que operan en sentido agravante, y que se han tenido en cuenta para fijar el importe de las dos multas:

- La vinculación de la actividad de la FSFA con la realización de tratamientos de datos personales (art. 83.2.k del RGPD y 76.2.b/ del LOPD DDD).
- El carácter continuado de la infracción (art. 83.2.ki 76.2.a LOPD GDD).
- La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance y propósito de la operación de tratamiento de que se trate, así como el número de personas interesadas afectadas (art. 83.2.a/). Se tiene aquí en consideración el número de personas trabajadoras afectadas por los accesos injustificados (24), así como el número de accesos llevados a cabo.

6. Por otra parte, de conformidad con el artículo 85.3 de la LPAC y tal y como se avanzó en el acuerdo de iniciación y también en la propuesta de resolución, si antes de la resolución del procedimiento sancionador la entidad imputada reconoce su responsabilidad o realiza el pago voluntario de la sanción pecuniaria, procede aplicar una reducción del 20% sobre el importe de la sanción provisionalmente cuantificada. Si concurren los dos casos mencionados, la reducción se aplicará de forma acumulada (40%).

Como se ha avanzado, la efectividad de dichas reducciones está condicionada al desistimiento o renuncia de cualquier acción o recurso por la vía administrativa contra la sanción (art. 85.3 de la LPAC, *in fine*).

Pues bien, tal y como se ha indicado en los antecedentes, la entidad imputada ha reconocido su responsabilidad y en fecha 04/03/2022 ha abonado de forma avanzada 6.000 euros (seis mil euros), correspondiente a la suma de las cuantías de las sanciones resultando una vez aplicada la reducción acumulada del 40% (4.800+1.200).

7. Ante la constatación de las infracciones previstas en el art. 83 del RGPD en relación con ficheros o tratamientos de titularidad privada, el artículo 21.3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, faculta a la directora de la Autoridad para que la resolución que declara la infracción establezca las medidas oportunas para que cesen o se corrijan sus efectos. En virtud de esta facultad, cabe decir lo siguiente:

7.1.- En relación con el hecho probado 1 y dadas las circunstancias concurrentes, no se considera procedente requerir la adopción de medidas correctoras, puesto que se trataría de unos hechos puntuales ya consumados.

7.2. En relación con el hecho probado 2, en concreto, en lo que se refiere a la utilización de unas mismas credenciales por varias personas para acceder al HC3 a través de la plataforma BSA, tampoco se considera procedente requerir la adopción de ninguna medida puesto que como se ha avanzado, la FSFA ya bloqueó el acceso al HC3 mediante dicha plataforma.

7.3. No obstante, se propone requerir a la FSFA para que lo antes posible y en todo caso en el plazo máximo de un mes a contar desde el día siguiente al de la notificación de la resolución, implemente en el sistema GENOMI (el aplicativo mediante el cual actualmente la FSFA puede acceder a las historias clínicas) las medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que permita garantizar la confidencialidad de los datos, y que incluya un proceso de verificación, evaluación y valoración regulares del eficacia de las medidas de seguridad implementadas (art. 32.1.d RGPD), como podría ser la exigencia de efectuar una revisión mensual de la información registrada sobre los accesos a las historias clínicas, con la elaboración del correspondiente informe.

Una vez adoptada la medida correctora descrita en el apartado 7.3 precedente en el plazo señalado, la FSFA informará a la Autoridad en el plazo de los 10 días siguientes, sin perjuicio de la facultad de inspección de esta Autoridad para efectuar las verificaciones correspondientes.

Por todo esto, resuelvo:

1. Imponer a la Fundación San Francisco de Asís dos sanciones consistentes en dos multas administrativas, una de 8.000 euros (ocho mil euros), como responsable de una infracción prevista en el artículo 85.5.a), en relación con el artículo 5.1.a); y, una multa de 2.000 euros (dos mil euros) por la infracción prevista en el artículo 85.4.a), en relación con el artículo 32, todos ellos del RGPD.
2. Declarar que la Fundación San Francisco de Asís ha hecho efectivo el pago adelantado de 6.000 euros (seis mil euros), que corresponde al importe total de las dos sanciones impuestas, una vez aplicado el porcentaje de deducción del 40% correspondiente a las reducciones previstas en el artículo 85 de la LPAC.
3. Requerir la Fundación San Francisco de Asís para que adopte la medida correctora señalada en el apartado 7.3 del fundamento de derecho 7º y acredite ante esta Autoridad las actuaciones llevadas a cabo para su cumplimiento.
4. Notificar esta resolución a la Fundación San Francisco de Asís.
5. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,