Identificación del expediente

Resolución de procedimiento sancionador núm. PS 32/2022, referente a la Fundación de Enfermos Mentales de Cataluña.

Antecedentes

1. En fecha 10/12/2020, tuvo entrada en la Autoridad una denuncia formulada por tres personas ((...), (...)y (...)) contra la Fundación de Enfermos Mentales de Cataluña (en adelante, FMMC), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales. En concreto, las personas denunciantes, (...), exponían los siguientes hechos que consideraban contrarios a la normativa, que tuvieron lugar en el mes de septiembre de 2020, en el seno de una auditoría de los sistemas de información entidad había encargado a una empresa externa contratada al efecto ((...)), y que habrían derivado en un " *incidente de seguridad (IN-061").*

a) Que (...)(...)((...)) había proporcionado a finales de agosto a (...) dos usuarios específicos (uno por cada auditor) con derechos de administración del sistema, con los que podían acceder remotamente vía VPN a los sistemas de la FMMC para realizar los trabajos de auditoría encomendados; pero estos usuarios se inhabilitaron cuando el citado responsable se marchó de vacaciones. Las personas denunciantes se quejan de que, ante esta circunstancia, la gerencia del FMMC, en vez de proceder a volver a habilitar a los usuarios específicos que se habían proporcionado en su día a los auditores, facilitó, sin conocimiento de las personas responsables de (...)(...)del FMMC, "el usuario genérico administrador" de dominio en (...), para que pudieran acceder con los máximos privilegios a los sistemas, como así hizo.

b) Que (...), sin conocimiento de los responsables de (...), y saltándose la seguridad perimetral del FMMC, instaló un " *hardware en las instalaciones para conectarse desde el exterior saltándose la seguridad del FMMC, y, mediante la contraseña del usuario Administrador, cedida por (...), poder realizar las tareas que necesitaran"* . Los denunciantes manifiestan que el protocolo de seguridad del FMMC prohíbe expresamente que mediante el usuario genérico administrador se pueda acceder remotamente al sistema, es decir, que *"este usuario especial sólo puede ser usado desde dentro de la red de la Fundación : por seguridad no puede ser usado para entrar desde fuera en los sistemas de la Fundación"* . En definitiva, los denunciantes afirman que, en la medida en que el sistema de seguridad implementado por el FMMC no permitía que a través del usuario administrador se pudiera acceder remotamente -a través de VPN (que era el sistema de acceso remoto previsto)- en los sistemas de información, (...) instaló dicho hardware para poder conectarse remotamente mediante el usuario administrador.

c) Que, a raíz *de "las intrusiones en los sistemas de información"* detectadas (por los denunciantes) por haber constatado accesos con el usuario administrador genérico, la gerencia, sin la intervención de los responsables (...) *"ordena a la empresa que realiza la auditoría (y presuntamente la autora de las intrusiones) a realizar una investigación ya cambiar las claves de todos los usuarios de la organización (...) gestionando así todas las credenciales de la organización y bloqueando el acceso de los usuarios en los sistemas al menos durante el fin de semana"* . A la vista de este bloqueo, las personas trabajadoras del

Generalitat de Catalunya

FMMC tuvieron que llamar a (...) para que esta empresa les facilitara una nueva contraseña para poder acceder a los sistemas. Las personas denunciantes afirman que en ningún momento se avisó al personal de que por seguridad debían proceder de forma inmediata a cambiar la contraseña proporcionada por (...). Es más, manifiestan que cuando advirtieron a (...) de este hecho, se les dijo *que "ellos no tenían esta práctica, que cada uno podía cambiar (la contraseña) cuando quisiera, que ellos eran profesionales y evidentemente nunca entrarían en la cuenta de un usuario".*

d) Que, durante el período durante el cual el sr. (...)no dispuso de acceso a los sistemas (en torno a la segunda quincena de septiembre de 2020 y hasta el 01/10/2020 en que lo recupera), *"hay pruebas de inicios de sesión en su equipo de trabajo y de accesos a software de gestión usando sus credenciales".*

Las personas denunciantes añadían que la gerencia del FMMC dirigió al "Código Tipo" de la Unión Catalana de Hospitales (UCH) -al que está adherido la Fundación-, una consulta sobre los hechos sucedidos para proceder a cerrar la incidencia, pero que la gerencia omitió información relevante al exponer el caso en la UCH.

Las personas denunciantes, junto con su denuncia aportaban la siguiente documentación:

- *"Informe incidencia de seguridad de fecha 18/09/2020",* elaborado el 29/09/2020 por el (...) quien, (...). Este informe contiene una cronología de los hechos que a su entender, habrían derivado en un incidente de seguridad (" *IN-061* "). Este informe, entre otros, incluye la copia de varios correos electrónicos intercambiados entre los responsables de (...)(...)((...) y (...)) y entre éstos y la gerencia de el FMMC.

- Copia de la respuesta que la UCH (Código tipo) dio al FMMC en relación con la consulta que la entidad le planteó relativa al incidente de seguridad. En este informe se recoge el siguiente literal:

"CONSULTA:
A raíz de unos hechos sucedidos tengo duda sobre la adecuación de dar por cerrada la incidencia de seguridad.
Se procedió a realizar una auditoría (...)para valorar la idoneidad de realizar una inversión en infraestructuras (...). Para que los auditores pudieran realizar su trabajo, se les habilitaron unos usuarios con acceso de administrador. Estos usuarios se deshabilitaron , y ante la necesidad de proseguir con la auditoría yo como (...) les di los códigos para acceder y que pudieran seguir haciendo la auditoría.
Ante estos hechos desde (...)(...)se envió un mail de alarma a toda la FMMC comunicando posibles ingresos indebidos en nuestra Red. Automáticamente aclaré que no eran accesos indebidos, sino accesos autorizados por mí, con la autorización también del Patronato, para poder proseguir con la auditoría no intrusiva.
Por mayor seguridad ordené a la empresa de auditoría que iniciaran una investigación y procedieran a cambiar todas las contraseñas tanto de administrador como de todos los usuarios. Finalizada la investigación se corroboró que no habían habido accesos no autorizados, sino los autorizados por mí como gerente.
Correctamente (...) analiza la situación, pero requiere un informe tanto por parte de Gerencia como de la empresa (...) y una posible comunicación a la Agencia.

Traducción automática

La consulta es si, habiendo comprobado que no ha habido accesos indebidos ni por tanto, fugas de información, es suficiente con mi información para cerrar la incidencia y no tener que destinar

RESPUESTA:
(...)
Del análisis anterior se puede concluir que:
1) La Entidad dispone de mecanismos que permiten detectar cuándo se producen incidencias.
2) Se ha abierto una incidencia con la voluntad de saber su origen y alcance.
Las explicaciones y actuaciones llevadas a cabo confirman que no se han producido accesos indebidos y por tanto, la incidencia ocurrida no tendría consideración de brecha de seguridad susceptible de tener que comunicarse a la autoridad de control pues no se ha ocasionado ni destrucción, ni pérdida, ni comunicación o acceso no autorizado a datos personales.
3) Las explicaciones y actuaciones llevadas a cabo permiten describir la incidencia y que ésta quede documentada de forma suficiente en el registro interno de la Entidad, no siendo requeridos informes adicionales salvo que los protocolos de la organización así lo dispongan específicamente.
4) En caso de que la Entidad valore reforzar alguna política de seguridad a raíz de la incidencia sucedida, pueden presentarse propuestas por parte de la Delegada de Protección de Datos, las cuales tendrán que ser aprobadas p(...)del tratamiento" .

2. La Autoridad abrió una fase de información previa (núm. IP 388/2020), 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 motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 21/01/2021 se requirió a la entidad denunciada para que diera cumplimiento a lo siguiente:

a) Informara si, tal y como se afirmaba en la denuncia, la gerencia del FMMC facilitó a (...) el usuario genérico administrador, que permite acceder a los sistemas con los máximos privilegios. En caso afirmativo, indicara qué razones organizativas y de urgencia habrían justificado que se facilitara a (...) el "usuario genérico administrador", en lugar de proceder a volver a habilitar a los usuarios específicos (que también tenían privilegios de administrador) que se habían proporcionado en su día a los auditores.

b) Informara si la gerencia del FMMC autorizó la instalación por parte de (...) de un hardware en la red del FMMC. En caso afirmativo, indicara si se autorizó el uso de este hardware para acceder a la red de la FMMC remotamente sin utilizar la VPN.

c) Informara si es cierto que, tal y como afirman las personas denunciantes, el sistema de seguridad perimetral del FMMC no permitía el acceso remoto por VPN mediante el usuario genérico administrador.

Traducción automática

d) Aportara el documento de evaluación de riesgos elaborado por la FMMC, y cualquier otro documento relativo a la seguridad de la información, vigente en las fechas en que ocurrieron los hechos denunciados (septiembre 2020).

e) En caso de haber contestado afirmativamente las preguntas a/ yb/, certificara que la gerencia del FMMC podía autorizar estas actuaciones (facilitar a (...) el usuario genérico administrador y autorizar la instalación y uso del hardware mencionado).

f) Confirmara o desmintiera el hecho denunciado en lo referente a que durante el período en que el (...) no tuvo acceso al sistema, alguien inició la sesión en su equipo de trabajo y accedió al software de gestión usando sus credenciales. De confirmarlo, indicara con detalle las razones que habrían justificado este acceso.

g) Aportara el contrato de encargado de tratamiento y cualquier documento que, a estos efectos, rigiera la relación contractual entre el FMMC y la empresa (...).

h) Aportara cualquier información adicional que estime procedente en relación con los hechos denunciados.

4. En fecha 31/01/2021 la entidad denunciada solicitó una ampliación de plazo para dar respuesta al requerimiento, que le fue concedida mediante acuerdo de 01/02/2021, notificado ese mismo día.

5. En fecha 09/02/2021, el FMMC respondió a dicho requerimiento a través de escrito en el que exponía lo siguiente:

- Que, efectivamente, la Gerencia *" facilitó a (...) el usuario genérico administrador que permite acceder a sistemas con los máximos privilegios".*

- Que *"(...)(...) dio accesos a los auditores pero los deshabilitó contraviniendo las instrucciones que explícitamente y por escrito se le habían indicado desde la Dirección".* Se detalla seguidamente la sucesión de hechos que, según el FMMC, propiciaron que a los auditores se les facilitara el usuario genérico administrador: la Gerencia *"informó al responsable (...)del FMMC ((...)) de la auditoría que se realizaría y se le pedía de forma precisa que fuera facilitador con los auditores en el marco de los servicios que tenían encomendados (...). Debido a un imprevisto, se tuvo que modificar la fecha fijada de realización de parte de los trabajos contratados por (...) y por tanto, las actuaciones serían llevadas a cabo mientras (...)(...)se encontraba de vacaciones. Conscientes de este hecho, la (...)lo comunica por escrito al responsable (...)precizándole que no debía quitar a los auditores los usuarios (...), instrucción que (...)(. ..)no cumple a pesar de contestarla afirmativamente. (...) A pesar de lo anterior, la realidad es que (...)(...) contravino la instrucción dada y dejó sin acceso a los auditores (...) La respuesta a la cuestión de porqué no se solicitó «volver a habilitar a los usuarios específicos que también tenían privilegios de administrador» es clara: (...) las razones organizativas y de urgencia que motivan facilitar a los auditores el usuario genérico de administrador responden a la desobediencia d(...)(...)junto con la necesidad de que los auditores contratados pudieran realizar su labor. Sobre este punto conviene indicar que el FMMC tenía a 3 personas incluidas en el usuario genérico de administrador: la (...), (...)(...)y (...)(...). Por tanto, siendo la (...)una de las personas con este usuario, optó por hacerlo*

Traducción automática

extensivo también a los auditores que necesitaban los máximos accesos para poder desarrollar la prestación encomendada en las fechas acordadas. Está claro que este usuario genérico de administrador se les facilitaba con carácter temporal (únicamente durante los trabajos que se realizaban) y con carácter excepcional y urgente (debido a la falta de acceso a través de los usuarios que se habían deshabilitado)" .

- Que *"las políticas de seguridad y protocolos de la entidad establecen que el usuario genérico de administrador no tiene acceso a la FMMC vía VPN. Esta previsión obedece a la definición de medidas de seguridad en escenarios cotidianos, que por situaciones excepcionales o debidamente motivadas, pueden verse alteradas. Se han descrito antes las razones que conducen a la realización de la auditoría de los expertos y las dificultades en que éstos puedan desarrollarla, explicando todo ello la no normalidad del momento que se vivía y que hace entender fácilmente que la aplicación del protocolo se viera modificada. A todo ello, se suma la situación generada por la pandemia de coronavirus en la que se estaba y está inmerso y la recomendación de llevar a cabo el máximo de las actuaciones de forma no presencial, que exige modular aspectos del día a día en la nueva realidad.*
  Lo anterior justifica pues que los auditores buscaran alternativas de acceso, ante la imposibilidad de hacerlo vía VPN. En este sentido, instalaron una máquina para realizar un escaneo de la red y detectar vulnerabilidades, tarea que se recuerda que estaba dentro de la prestación contratada. La Dirección y el Patronato estaban enterados de las actuaciones, las cuales autorizaban para que, tal y como habían explicado los auditores "el nuevo sistema de acceso remoto mantenía igualmente todas las garantías de seguridad, pues el tráfico viajaba de forma cifrada punto a punto" .

- Que " *se confirma que el usuario genérico de administrador no permitía el acceso remoto por VPN. Este punto va estrechamente ligado a las explicaciones dadas"* en el punto precedente.

- Que " *en cuanto a la seguridad de la información y en general, el cumplimiento de la normativa de protección de datos, interesa destacar que la Fundación siempre ha sido proactiva y ha tenido especial sensibilidad en esta materia (...)". En este sentido, el FMMC ya dispone del análisis de riesgos de los tratamientos descritos en el RAT, también de las evaluaciones de impacto de algunos de ellos".*

- Que la gerencia *"podía autorizar las actuaciones descritas en los puntos"* a/ yb/ del requerimiento de esta Autoridad (antecedente 3º), de acuerdo con lo que *"se dispone en los artículos 17 y 24 de los estatutos, y en los poderes que le fueron otorgados. Anexo 6, se aporta copia de los estatutos y escritura de agosto de 2020"* otorgada ante notario.

- *Que "las actuaciones llevadas a cabo por parte de los auditores externos provocaron una alerta al responsable (...) ((...)). En efecto, la alerta conllevó que el (...) cruzara comunicaciones con (...)(...)(que en aquellos momentos estaba de vacaciones) en relación a los accesos a los servidores de la Fundación pero en cambio, no contactó en ningún momento con la (...)(que no estaba de vacaciones, sino plenamente operativa), a pesar de ser una cuestión de seguridad de máxima relevancia.(...). En paralelo, también el 18 de septiembre a las 8:48h el (...) envía un comunicado a toda la Fundación bajo el título «intrusiones en los sistemas de la Fundación» en el que se informa de los accesos desconocidos a los servidores de la Fundación.(...) Inmediatamente después de esto, la*

Traducción no oficial

(...)a las 10:06 envía a toda la Fundación un mensaje en el que explica que los accesos habían sido previstos y autoridades por ella en el marco de la auditoría (...)que se estaba realizando en el FMMC. (...) A pesar de que desde la Dirección se creía que los accesos producidos en el servidor sólo eran los autorizados a los auditores, para confirmarlo y gestionar correctamente la incidencia, se abre una investigación. Dentro de las actuaciones, como medida de seguridad, se procede a cambiar las contraseñas de todos los usuarios. Esto se explica en el correo electrónico que la (...) envía a las 14:49h a todo el mundo. (...) Es justamente durante el proceso de bloqueo de todas las comunicaciones, fruto del supuesto ataque ya requerimiento de la dirección del FMMC, que los auditores externos detectan al menos dos máquinas con programas de control remoto residentes accesibles desde internet . Uno de los equipos se encuentra ubicado en el despacho del departamento (...), por tanto, se cree oportuno acceder al equipo del (...) respondiendo a la necesidad de certificar la inexistencia de este tipo de software instalado en su propio perfil que pudiera suponer una vulneración de la seguridad al permitir conexiones remotas. Por tanto, se concluye que temporalmente los accesos que el (...) tiene suspendidos quedan en manos de los auditores porque tienen la instrucción de verificar que no se hayan producido accesos no autorizados ni se haya puesto en riesgo la información o seguridad de la Fundación".

- Que se aporte el contrato de encargado del tratamiento con la empresa auditora.

- Que *"desde el FMMC entendemos que estamos ante una situación de conflicto ajeno a la normativa de protección de datos. Efectivamente esta denuncia se produce en un contexto ligado a la pérdida de confianza de la entidad FMMC con determinados mandos intermedios ((...), (...)y (...)(...)) (.. .) …). (...)(…)"*

- Que *"hay que hacer referencia a que gran parte del contenido de la denuncia gira en torno a si las decisiones fueran adoptadas por quien tenía esta competencia y/o encomendada la función (...). Por tanto, en el marco de la gestión y correcto desarrollo de la actividad fundacional, queda bajo el control de la Dirección General la ejecución de las decisiones del Patronato (máximo órgano de gobierno) y la adopción de las órdenes o contraórdenes sobre acciones que mandos intermedios pudieran realizar. A lo anterior se suma que en los últimos tiempos había desconfianza en la persona que ostentaba el rol de responsable (...)*

- Que, *"por último pero no menos importante, incidir en la época de coronavirus en la que vivimos. Desde la declaración de estado de alarma en marzo de 2020, las entidades han tenido que seguir adelante adaptándose de forma imprevista a nuevos retos sin dejar en ningún momento la actividad, sobre todo en instituciones con carácter asistencial como lo es 'FMMC'.*

La entidad denunciada aportaba con su escrito diversa documentación, entre otros:

i. Copia de varios correos electrónicos enviados por la gerencia al (...): 1) correo de 28/08/2020 en el que gerencia le informa que se ha encargado una auditoría interna a la empresa (...), así como de las fechas en que se lleva a cabo, 2) correo de 02/09/2020 en el que le informa que la auditoría se retrasa una semana y le pide que no inhabilite a los usuarios inicialmente asignados a los auditores.

Traducción automática

ii. Copia del correo electrónico enviado el 14/09/2020 por uno de los auditores a la gerencia en la que informaba de que no podía entrar en el sistema porque su usuario estaba inhabilitado.

iii. Copia del correo electrónico que el 18/09/2020 a las 8:48 el (...) habría enviado a todo el personal exponiendo que *"se han constatado accesos no autorizados a los servidores de la Fundació. Esto ha originado una incidencia de seguridad. Parece que no hay daños (...)".*

iv. Copia de los correos electrónicos que la gerencia habría enviado el 18/09/2021 a todo el personal: 1) correo de las 10:06 en que, haciendo referencia al correo electrónico que había enviado el (...) ese mismo día, informaba que *"las intrusiones estaban previstas y autorizadas por mí para finalizar la Auditoría (...)visual y no intrusiva que se está realizando (...)",* 2) correo de las 14:49 en que se informaba al personal que se procedería a cambiar los passwords y contraseñas de VPN, que no podrían acceder con la contraseña actual, y que era necesario llamar a la empresa de auditoría (...) para obtener una nueva.

v. Contrato entre la FMMC y(...), fechado el 28/08/2020 y firmado por las partes en la misma fecha, para la realización de una auditoría interna preventiva, que contendría las previsiones establecidas en el artículo 28 de 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) , en cuanto al encargo del tratamiento.

vi. Certificado emitido por el Código Tipo de la UCH, en el que certifica que durante 2020 el FMMC ha llevado a cabo diversas actuaciones que acreditan que la entidad cumple los requisitos básicos exigidos para estar adheridos a la organización. En concreto, certifica la asistencia a sesiones formativas plenarias y monográficas ofertadas a entidades adheridas al Código Tipo, realización de sesiones formativas a sus profesionales, realización de dos evaluaciones de impacto y realización de auditorías en protección de datos.

vii. Copia de los estatutos del FMMC, cuyo artículo 23 dispone que el Patronato *"nombrará a un Director-Gerente de la Fundación, (...) al que le serán asignadas las funciones que se establezcan en el acuerdo de nombramiento, referidas principalmente en la administración y gestión de la Fundación".*

viii. Copia de la escritura de otorgamiento de poderes por parte del FMMC en la actual gerencia, de fecha 05/08/2020. En este documento se recoge el acuerdo adoptado por Patronato de la Fundación de fecha 22/06/2020 mediante el cual se confiere poder a favor de (...) *"para que en nombre y representación de la Fundación, pueda ejercer las facultades que constan en la certificación protocolizada a la que me remito".* Esta certificación, unida a la escritura, recoge de forma detallada los amplios poderes otorgados por el FMMC a la (...), entre otros, las *"facultades de gestión y administración"* entre las que se incluye *"1) Administrar los bienes de la fundación y llevar la dirección y gestión de las actividades propias de la Fundación, sus derechos y obligaciones, con facultad para realizar y otorgar toda clase de actos, operaciones, contratos y otros*

Traducción al Alemán

documentos (...) 5) Nombrar y despedir a trabajadores, fijando sus atribuciones, sueldos y emolumentos (...)" .

6. En fechas 09/03/2021 y 24/03/2022, aún en el seno de esta fase de información previa, se dirigieron sendos requerimientos al FMMC para que ampliaran alguna de las respuestas que dieron mediante el suyo escrito de 09/02/2021; en concreto:

- Informar de las circunstancias que explicarían que los auditores externos conocieran las credenciales personales de acceso del (...) a los sistemas de información del FMMC, y mediante las cuales los auditores habrían accedido a su equipo de trabajo.

- Confirmara si, tal y como afirmaban las personas denunciantes, cuando las personas trabajadoras del FMMC accedieron al sistema por primera vez mediante la nueva contraseña proporcionada por (...), el sistema no les forzó a cambiarla.

7. En fechas 19/03/2021 y 05/04/2022 el FMMC dio respuesta a los anteriores requerimientos de información, exponiendo lo siguiente:

a) Que " *se confirma que los auditores tenían usuario genérico de administrador. Fue con este usuario de administrador que cambiaron la contraseña del (...) para poder acceder a su perfil de usuario. Por tanto, los auditores no conocían las credenciales personales de acceso del (...), de las que nunca hicieron uso, sino que actuaron siempre con las credenciales de administrador para acceder a los sistemas de información de la Fundación.*
Se quiere volver a destacar que el acceso al equipo del (...) era necesario para poder verificar que no hubiera ningún software de acceso remoto instalado como se había detectado ya en otros 2 equipos (el de la sala de juntas y el de la sala (...)de información), los cuales se deshabilitaron para minimizar riesgos".

b) Que " *Se confirma que para realizar el cambio de la contraseña, los trabajadores llamaban a (...) y les daba una nueva contraseña. En el momento de dársela, (...) informaba de la necesidad de que la primera vez que accedieran había que hacer el cambio de la contraseña y que ésta no coincidiera con una antigua.*
El cambio de la contraseña por parte del trabajador pero sólo venía impuesto por el sistema por aquellos trabajadores que en ese momento estaban en las oficinas de la Fundación. En cambio, para los trabajadores que estaban teletrabajando, este cambio debía realizarlo el propio trabajador porque técnicamente a través de la VPN no era posible que fuera obligatorio. Es precisamente por este motivo que (...) explicaba a cada trabajador la necesidad de realizar el cambio de contraseña en el momento que se les llamaba por teléfono para pedir la contraseña".

8. A petición del Área de Inspección, la Coordinación de Tecnología y Seguridad de la Información de la Autoridad analizó los hechos objeto de denuncia, análisis recogido en un documento de fecha 22/04/2022.

9. En fecha 26/05/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el FMMC por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 32; ambos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las

Traducción automática

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 30/05/2022.

10. El acuerdo de iniciación explicitaba los motivos por los que no se efectuó imputación alguna respecto de otros hechos denunciados. En primer lugar, en lo que se refiere al acceso al equipo de trabajo de una de las personas denunciantes por parte de los auditores, se archivó en la medida en que en el marco de las investigaciones no se pudo constatar que, atendidas las circunstancias concurrentes, dicho acceso no fuese necesario para garantizar la seguridad del sistema informático de la FMMC. Y, en segundo lugar, en cuanto a la facilitación por parte de la gerencia a los auditores externos de un usuario genérico administrador y que se les autorizara la instalación en los sistemas de información de la entidad de un hardware que permitiera la conexión remota sin utilizar el VPN, se archivó ya que estos hechos por sí mismos no tendrían la entidad suficiente como para alojarse en una vulneración de medidas de seguridad. Además, se puso de relieve que los auditores siguieron en todo momento las instrucciones dadas por la gerencia quien, de acuerdo con la documentación proporcionada por la entidad en el marco de las investigaciones, tenía la facultad para tomar este tipo de decisiones, de acuerdo con los amplios poderes que le había conferido el FMMC.

11. 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.

1 **2.** En fecha 07/06/2022 el FMMC solicitó la ampliación del plazo para formular alegaciones, lo que se le concedió mediante acuerdo de 07/06/2022 notificado el mismo día.

13. En fecha 17/06/2022, el FMMC presentó un escrito en el que reconocía su responsabilidad en los hechos imputados, y reiteraba lo expuesto en el marco de la información previa en relación con las circunstancias que habían propiciado los hechos imputados. En el mismo escrito el FMMC relacionaba aquellas circunstancias que a su juicio justificarían *"una minoración al máximo de la sanción que corresponda imponer".*

Junto a este escrito, la entidad imputada aportaba el documento acreditativo de su adhesión al Código Tipo de la Unión Catalana de Hospitales.

14. En fecha 12/07/2022, la instructora de éste procedimiento formuló una propuesta de resolución , por la que proponía que la directora de la Autoridad Catalana de Protección de Datos impusiera al FMMC con una multa administrativa de 2.500 euros (dos mil quinientos euros) como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 15/07/2022 y se concedía un plazo de 10 días para formular alegaciones.

15. En fecha 19/07/2022 el FMMC ha presentado un escrito en el que no formula alegaciones y acredita el pago por adelantado de la cantidad de 1.500 euros (mil quinientos euros), correspondientes a la sanción pecuniaria propuesta por la instructora en la propuesta de resolución, una vez aplicadas las reducciones previstas en el artículo 85 de la LPAC (en

traducción automática

este punto cabe recordar que en el escrito de 17/06/2022 -antecedente 13- la entidad reconoció la responsabilidad en los hechos imputados). Por otra parte, junto con su escrito, el FMMC aporta un certificado emitido por la gerencia del FMMC en el que manifiesta que *"todo aquel personal al que los auditores facilitaron una contraseña de acceso a los sistemas de información de la entidad, el sistema informático les ha forzado a cambiarla por otra personal e intransferible"* , certificado que había sido propuesto por la instructora como medida correctora en la propuesta de resolución.

Hechos probados

En el marco de la realización de una auditoría interna de los sistemas de información, las personas auditoras contratadas por el FMMC, con el conocimiento y autorización de la gerencia, en fecha indeterminada, pero en todo caso comprendida entre el 18/09 /2020 y el 30/09/2020, llevaron a cabo las siguientes actuaciones:

- Por razones de seguridad, se procedió a inhabilitar las contraseñas del personal del FMMC para acceder a los sistemas de información. Con el fin de obtener las nuevas credenciales de autenticación, el personal debía contactar con la empresa auditora, quien era la encargada de proporcionarlas. El proceso de asignación de las nuevas contraseñas -descrito por la misma entidad (apartado b/ del antecedente 7º) era el siguiente *: "(...) los trabajadores llamaban a (...) y les daba una nueva contraseña . En el momento de dársela, (...) informaba de la necesidad de que la primera vez que accedieran había que hacer el cambio de la contraseña y que ésta no coincidiera con una antigua. El cambio de la contraseña por parte del trabajador pero sólo venía impuesto por el sistema por aquellos trabajadores que en ese momento estaban en las oficinas de la Fundación. En cambio, para los trabajadores que estaban teletrabajando, este cambio debía realizarlo el propio trabajador porque técnicamente a través de la VPN no era posible que fuera obligatorio. Es justamente por este motivo que (...) explicaba a cada trabajador la necesidad de realizar el cambio de contraseña en el momento que se les llamaba por teléfono para pedir la contraseña"* .

En este proceso descrito de asignación de las nuevas contraseñas, no se establecieron las medidas de seguridad oportunas que garantizaran que la contraseña fuera conocida únicamente por el usuario correspondiente (como sería forzar al usuario al cambio de contraseña en su primer acceso al sistema).

- Una vez se inhabilitaron las credenciales del (...), Responsable (...) -como al resto del personal-, los auditores, con el usuario genérico administrador, procedieron a asignarle unas nuevas credenciales, y fue mediante estas nuevas credenciales vinculadas al (...) que los auditores accedieron a su equipo de trabajo. Este acceso, según informó el FMMC, se limitó a verificar que en dicho equipo no se había instalado ningún software de acceso remoto que pusiera en peligro la seguridad del sistema.

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

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.

El tratamiento de datos denunciado recae dentro del ámbito competencial de la Autoridad en virtud de lo previsto en el artículo 156.b) del Estatuto de Autonomía de Cataluña (EAC) y el artículo 3.h) de la Ley 32/2010, dado que el FMMC es una entidad proveedora de la Red de Servicios Sociales de Atención Pública, y presta servicios públicos por cuenta del Departamento de Derechos Sociales de la Generalidad de Cataluña.

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.

Tal y como se ha adelantado a los antecedentes, la entidad imputada no ha formulado alegaciones en el seno de este procedimiento sancionador, acogiéndose a ambas opciones para reducir el importe de la sanción, reconociendo su responsabilidad en los hechos imputados y pagando por adelantado el importe de la sanción propuesta por la instructora a la propuesta de resolución (con la reducción correspondiente del 40%).

Sin embargo, se considera oportuno reiterar aquí las apreciaciones hechas por la instructora sobre las circunstancias que, según el FMMC, habrían propiciado los hechos imputados en el procedimiento, invocando especialmente la situación de pandemia que se vivía en aquellos momentos, que comportó que la organización tuviera que adaptarse a nuevas situaciones de gestión de recursos humanos hasta aquellos momentos nunca vividas, y poniendo de relieve que en todo momento su actuación había sido destinada a evitar eventuales vulnerabilidades en sus sistemas de información.

Al respecto, cabe decir que esta Autoridad es conocedora de las difíciles circunstancias que se dieron en entidades, como la aquí imputada, en las fechas en que ocurrieron los hechos denunciados (septiembre de 2020), en plena pandemia de COVID; y entiende que esta situación requirió un sobreesfuerzo adicional por parte de todas las organizaciones; pero dicho esto también cabe remarcar que esta situación de excepcionalidad no puede amparar la vulneración de la normativa de protección de datos, en este caso, la falta de implementación de medidas de seguridad adecuadas al riesgo.

3. En relación con las conductas descritas en el apartado "Hechos Probados", relativas 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, (.. .)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;*

Resolución automatizada

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 las datos personales de forma rápida en caso de incidente físico o técnico;*
d) *un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*
2. *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichas datos.*
3. *La adhesión a un código de conducta aprobado a tenor del artículo 40 oa 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. *(...) y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad de (...)o del encargado y tenga acceso a datos personales solo pueda tratar dichas datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del derecho de la Unión o de los Estados miembros".*

Como se ha dicho, respecto a las conductas descritas en el apartado de hechos imputados, se considera que el FMMC ha vulnerado las medidas de seguridad que se detallan a continuación:

De acuerdo con lo dispuesto en la disposición adicional primera de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), cabe mencionar lo que establecen los apartados 4.2. 1 y 4.2.5 del Anexo II ("Medidas de Seguridad") del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), vigente cuando ocurrieron los hechos:

"4.2.1 Identificación [op.acc.1]_

dimensiones	AT		
nivel	bajo	medio	alto
	aplica	=	=

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.

2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los

Traducción automática

sistemas) recibirá identificadoras singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad .

3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:
a) Se puede saber quién recibe y qué derechos de acceso recibe.
b) Se puede saber quién ha hecho algo y qué ha hecho.

4. Los cuentas de usuario se gestionarán de la siguiente forma:
a) Cada cuenta estará asociada a un identificador único.
b) Los cuentas deben ser inhabilitados en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la que se requería el cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.
c) Los cuentas se retendrán durante el período necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este período se le denominará período de retención.
(…)

4.2.5 Mecanismos de autenticación [op.acc.5]

dimensiones	ICAT		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que sean, pudiendo usarse los siguientes factores de autenticación:
– "algo que se sabe": contraseñas o claves concertadas.
– "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
– "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de forma aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación en los que se utilicen sistema se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, éstos deberán haberse identificado y registrado de forma fidedigna ante el sistema o ante un proveedor de identidad electrónico reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:
– Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
– De forma telemática, mediante DNI electrónico o un certificado electrónico calificado.

Traducción automática

– De forma telemática, utilizando otros sistemas legalmente admitidos para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO
a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma .
c) Se atenderá a la seguridad de las credenciales de forma que:
1. Las credenciales se activarán una vez extendido bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentiquen termina su relación con el sistema.

Nivel MEDIO
a) Se exigirá el uso de al menos dos factores de autenticación.
b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.
c) Las credenciales utilizadas habrán sido obtenidas tras un registro previo:
1. Presencial.
2. Telemático usando certificado electrónico calificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico calificado en dispositivo calificado de creación de firma.

Nivel ALTO
a) Las credenciales se suspenderán tras un período definido de no utilización.
b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Las credenciales utilizadas habrán sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico calificado en dispositivo calificado de creación de firma".

Así, poder establecer de forma clara la trazabilidad de los accesos (quien, cuándo, a qué información, etc), resulta una medida necesaria para asegurar la protección de la información objeto de tratamiento; lo que no ocurría en el caso analizado en el que, tal y como se ha expuesto en el apartado de hechos probados, no se garantizó que las credenciales de acceso al sistema estuvieran siempre bajo el control exclusivo de los usuarios (medida op.acc .5); ya que, una vez suministradas las nuevas contraseñas a los usuarios, no se estableció un sistema o protocolo por el que éstos debieran cambiarla necesariamente en su primer acceso al sistema informático. Asimismo, en la medida en que las contraseñas no estuvieron bajo el control exclusivo de los usuarios, también resultó afectada la medida especificada en el op.acc.1, ya que a partir de ese momento ya no sería

Traducción automática

posible establecer de forma indudable quién, qué y cuándo se ha hecho una determinada actuación dentro del sistema, lo que resulta especialmente claro en el caso de la persona que ocupaba el cargo de Responsable (...), en la que los auditores accedieron a su equipo de trabajo utilizando unas nuevas credenciales que éstos le asignaron "ex novo ".

Durante la tramitación de este procedimiento se ha acreditado debidamente los hechos descritos en el apartado de hechos probados, que se consideran constitutivos de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica 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.

Las conductas que aquí se abordan se han 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 ".*

4. Al no meterse el FMMC 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 83.4 del RGPD contempla una sanción de multa hasta un máximo de 10.000.000 de euros, 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. Esto, sin perjuicio de que, con carácter adicional o sustitutivo, se pueda aplicar alguna otra de las medidas previstas en el artículo 58.2 RGPD.

En el presente caso, tal y como exponía la persona 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 la falta de control sobre las contraseñas afectó a numerosas personas trabajadoras de la entidad y, en consecuencia, en relación con todas estas personas no pudo establecerse de forma clara la trazabilidad de los accesos al sistema de información del FMMC.

Descartado que proceda sustituir la sanción de multa administrativa por una amonestación, corresponde determinar la cuantía de la 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 la sanción de 2.500 euros (dos mil quinientos euros). Esta cuantificación de la multa se basa en la ponderación entre los criterios agravantes y atenuantes que a continuación se indican.

Como criterios atenuantes, se observa la concurrencia de las siguientes circunstancias, todas ellas invocadas por el FMMC:

Traducción automática

- 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 que no se tiene constancia de ningún acceso indebido por parte de los auditores (únicos que conocían las contraseñas de las personas trabajadoras) a los sistemas de información, y que los hechos objeto de imputación derivaron de una actuación puntual y aislada en el tiempo (83.2.a RGPD).

- La falta de intencionalidad (art.83.2.b RGPD).

- La adhesión por parte del FMMC al código de conducta de la Unión Catalana de Hospitales (art. 83.2.j RGPD).

- La falta de constancia de la obtención de beneficios como consecuencia de la infracción (art. 83.2.k RGPD y 76.2.c LOPDGDD).

- La naturaleza de la entidad de Fundación privada sin ánimo de lucro -art. 1 de sus Estatutos- (art. 83.2.k RGPD).

- Que en los dos últimos ejercicios contables la FMMC ha tenido pérdidas (art. 83.2.k RGPD).

Por el contrario, no puede tener en cuenta otras circunstancias atenuantes invocadas por la entidad, por las razones que seguidamente se exponen:

- Grado de cooperación con la autoridad de control. Al respecto cabe decir que el mero hecho de haber contestado los requerimientos de esta Autoridad en la fase de información previa, no justificaría la aplicación del atenuante prevista en la letra f) del artículo 83.2; esencialmente porque contestar a dichos requerimientos es una obligación de las entidades sujetas a su ámbito de actuación (artículo 19 de la Ley 32/2010) y al no hacerlo puede ser constitutivo de infracción.

- Carácter no continuado de la infracción. El FMMC aboga por la aplicación de este atenuante (76.2.a LOPDGDD) ya que su actuación fue un "error puntual". Al respecto cabe decir que el hecho de que se tratara de una actuación puntual en el tiempo es una circunstancia que ya se ha tenido en cuenta en el primero de los atenuantes relacionados en el apartado anterior -art. 83.2.a RGPD-.

- La carencia de infracciones anteriores en materia de protección de datos. Respecto a esta circunstancia cabe decir que no puede aplicarse como criterio atenuante, ya que es obligación de las entidades que tratan datos personales cumplir con la normativa; por lo que si concurriera tal circunstancia -que no es el caso- actuaría como criterio agravante.

- Actuación del FMMC *"rápida y eficaz",* tendente a evitar *"un escape de datos",* circunstancia que el FMMC encabeza en la circunstancia prevista en el artículo 83.2.c) del RGPD [" *cualquier medida tomada por el responsable u encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados"]* . Este criterio atenuante sería de aplicación cuando la entidad hubiera llevado a cabo actuaciones para paliar los efectos o perjuicios de la infracción cometida, y el FMMC no se refiere a actuaciones

Traducción automática

tomadas en este sentido, sino que lo que hace es explicar el porqué va a llevar a cabo las actuaciones que, como se ha visto, supusieron la vulneración de medidas de seguridad que son, precisamente, las que han derivado en la incoación de este procedimiento sancionador.

En contraposición a las causas atenuantes expuestas, concurre el siguiente criterio que opera en sentido agravante, y que se ha tenido en cuenta para fijar el importe de la multa.

- La vinculación de la actividad de la FMMC con la realización de tratamientos de datos personales (art. 83.2.k del RGPD y 76.2.b/ de la LOPDGDD).

5. Por otra parte, de conformidad con el artículo 85.3 de la LPAC y tal y como se adelantaba al acuerdo de iniciación y también a 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 vía administrativa contra la sanción (art. 85.3 de la LPAC, *in fine*).

Pues bien, tal y como se ha indicado en los antecedentes, mediante escrito de 17/06/2022, la entidad imputada reconoció su responsabilidad. Asimismo, en fecha 19/07/2022 ha abonado de forma avanzada 1.500 euros (mil quinientos euros), correspondientes a la cuantía de la sanción resultante una vez aplicada la reducción acumulada del 40%.

6. Ante la constatación de las infracciones previstas en el art. 83 del RGPD en relación con ficheros o tratamientos efectuados por entidades no incluidas en el artículo 77.1 del LODGDD, 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. Sin embargo, en el presente caso no es necesario requerir la adopción de ninguna medida correctora ya que la entidad en el seno de este procedimiento ha llevado a cabo la medida propuesta por la instructora, consistente en certificar que *"todo aquel personal a quien les auditores facilitaron una contraseña de acceso a los sistemas de información de la entidad, el sistema informático les ha forzado a cambiarla por otra personal e intransferible"* .

Por todo esto, resuelvo:

1. Imponer a la Fundación de Enfermos Mentales de Cataluña la sanción consistente en una multa de 2.500 euros (dos mil quinientos euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32 , ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 6º.

Traducción automática

2. Declarar que la Fundación de Enfermos Mentales de Cataluña ha hecho efectivo el pago adelantado de 1.500 euros (mil quinientos euros), que corresponde al importe total de la sanción impuesta, una vez aplicado el porcentaje de deducción del 40% correspondiente a las reducciones previstas en el artículo 85 de la LPAC.

3. Notificar esta resolución a la Fundación de Enfermos Mentales de Cataluña.

4. 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 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,

Traducción automática