apdcat
Autoritat Catalana de Protecció de Dades

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

Identificación del expediente

Resolución del procedimiento sancionador núm. PS 19/2018, en lo referente al Instituto Catalán de la Salud.

Antecedentes

1.- En fecha 27/10/2017 tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito por el que se formulaba denuncia de una persona contra el Instituto Catalán de la Salud (en adelante ICS), con motivo de un presunto incumplimiento de la normativa de protección de datos. En concreto, la persona denunciante -usuaria del CAP (...), SAP (...)- exponía que personas no autorizadas habrían accedido a su historia clínica sin su consentimiento. Para acreditar los hechos denunciados, la persona afectada (de quien el ICS ha conocido la identificación en la fase de información previa), aportaba la siguiente documentación:

a) Documento titulado "Listado de accesos desde el 01/11/2016 hasta el 15/08/2017". En este listado constan varios accesos a la historia clínica de la persona denunciante el día 27/03/2017, por parte de una persona con la categoría profesional de "auxiliar administrativo" quien prestaría servicios en el CAP (...). En concreto constan los siguientes accesos:

• Módulo "USUFG005 –Mantenimiento de usuarios y pacientes" a las 11:07
• Módulo "USUG068 Etiquetas por usuario" a las 11:07 •
Módulo "USUG068 Etiquetas por usuario" a las 11:07 •
Módulo "USUFG005 –Mantenimiento de usuarios y pacientes" a las 12:48

Estos cuatro accesos pueden reducirse a dos, en la medida en que tres de ellos se produjeron a la misma hora (11:07).

b) Oficio de fecha 31/08/2017, que el EAP (...) dirigió a la persona denunciante. En este escrito se le informaba que no se había constatado que los accesos indicados en el apartado anterior "estén ligados a visitas profesionales sanitarias", y que este hecho se había puesto en conocimiento de la dirección del SAP (...).

2.- La Autoridad abrió una fase de información previa (núm. IP 340/2017), de acuerdo con 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), a fin de determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes concurrentes en unos y otros.

En el seno de esta fase de información, por medio de oficios de fechas 11/12/2017 y 09/01/2018 (este último reiterado el 17/01/2018 y el 21/02/2018) se requirió el ICS para que diera cumplimiento a lo siguiente:

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

- Identificara a la persona a la que corresponderían los dos accesos controvertidos a la historia clínica de la persona aquí denunciante y confirmara que el día 27/03/2017 esta persona prestaba servicios como auxiliar administrativo en el CAP (...).
- Confirmara si, tal y como apuntaba el EAP (...) en su oficio de 31/08/2017, los accesos indicados no respondían a ninguna razón asistencial.
- Informara si el ICS había iniciado una información reservada sobre los accesos controvertidos. En caso afirmativo, aportara una copia de la documentación que allí figure.
- Indicara qué razón sanitaria/asistencial justificaría que personas con un perfil de usuario vinculado a un determinado CAP puedan acceder a las historias clínicas de pacientes usuarios/as de otro CAP. En relación con estos casos (acceso por parte de un/a usuario/a vinculado a un CAP a historias clínicas de pacientes asignados a otro CAP) informara sobre lo siguiente:

    • Si el sistema informático alerta de algún modo al usuario/a que accederá a la historia clínica de un paciente vinculado a otro CAP.
    • Si, para acceder a la historia clínica, el usuario debe indicar forzosamente las razones que justificarían este acceso.
    • Si estos tipos de acceso son analizados expresamente por el responsable de seguridad y si éstos se reflejan en el informe mensual que debe elaborarse de acuerdo con lo que prevé el artículo 103.5 del Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RLOPD y LOPD).

- Aportara el informe mensual elaborado por el responsable de seguridad, en el que se analicen las revisiones efectuadas, y los eventuales problemas detectados en el mes de marzo de 2017.

El ICS respondió a los anteriores requerimientos a través de escritos de fechas 02/01/2018, 16/01/2018 y 23/02/2018, por los que se exponía, entre otros, lo siguiente:

- Que Dª. (...) (persona a quien correspondería el usuario quien efectuó los accesos controvertidos) prestaba servicios el día 27/03/2017 como auxiliar administrativo en el CAP (...).
- Que "los accesos no son asistenciales" y se realizan "desde el perfil de ECAP administrativo".
- Que la Gerencia Territorial Cataluña Central, mediante escrito de fecha 31/10/2017, solicitó "autorización para tramitar una información reservada, a fin de averiguar si los accesos mencionados a la historia clínica de Dª. (nombre de la persona denunciante) están justificados (...)". Que posteriormente el ICS "ordenó la realización de una información reservada por parte del área de Apoyo Jurídico Laboral y Normativo de la propia Gerencia".

- Que "el vínculo por el que un trabajador con perfil de usuario no sanitario de la ECAP Administrativo tiene con un CAP concreto se establece por motivos de gestión de agendas, de programación de visitas y de otras tareas meramente administrativas".
- Que "la razón asistencial por la que una persona con perfil de usuario no sanitario de la ECAP Administrativo vinculado a un CAP determinado puede acceder a datos administrativos de cualquier ciudadano, aunque no pertenezca o tenga médico asignado en este mismo

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

CAP, pero que sí pertenece a la propia Gerencia Territorial, es la consecución de un buen servicio a la ciudadanía".

- Que las personas con un perfil de usuario vinculado a un determinado CAP que no pertenece a una misma Gerencia Territorial "no pueden acceder (a las historias clínicas de pacientes) si previamente no se han recuperado los datos del paciente desde el ECAP Administrativo. Entonces el profesional asistencial tendrá acceso a los datos clínicos de este paciente que estén publicados en el HC3. Este hecho se daría, por ejemplo, cuando un paciente adscrito a una Gerencia territorial acude, por el motivo que sea, a una visita a otro centro de otra Gerencia territorial. En caso de que no se produjera este hecho, el profesional del centro de Gerencia diferente a la adscripción del usuario sólo podría acceder a pocos datos (nombre, apellidos, DNI, NASSS, CIP, dirección y teléfono), nunca de tipo clínico".

- Que el sistema no da ninguna alerta en caso de acceder a una historia clínica de un paciente vinculado a otro CAP, pero que "el usuario lo ve porque el paciente no tiene médico asignado en el centro en el que se encuentran" .
- Que "no se considera necesario" que el usuario, para acceder a la historia clínica de un paciente vinculado a otro CAP, indique las razones de dicho acceso.
- Que este tipo de accesos no son analizados expresamente por el responsable de seguridad y por tanto "no se reflejan en ningún informe".

3.- En fecha 18/07/2018, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el ICS, en primer lugar, por una presunta infracción grave prevista en el artículo 44.3.d) en relación con el artículo 10 de la LOPD; y, en segundo lugar, por una presunta infracción también grave prevista en el artículo 44.3.h) en relación con el artículo 9 de la LOPD. Asimismo, nombró persona instructora del expediente a la señora (...), funcionaria de la Autoridad Catalana de Protección de Datos.

5.- Este acuerdo de iniciación se notificó a la entidad imputada en fecha 23/07/2018.

6.- En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles a contar a partir del día siguiente de la notificación, para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

7.- En fecha 25/07/2018, el ICS formuló alegaciones en el acuerdo de iniciación. En sus alegaciones, centradas únicamente en el primero de los hechos que se declaran probados en este procedimiento, el ICS esgrimía que los accesos controvertidos estaban justificados por "motivos organizativos", y añadía que únicamente se habría accedido a "datos administrativos , no asistenciales".

8.- Ante las alegaciones formuladas, por Acuerdo de fecha 04/10/2018 la persona instructora dispuso la apertura de un período de prueba, con el fin de practicar en el plazo de 10 días a contar desde el día siguiente a la notificación, las pruebas consistentes en:

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

- Que el ICS informara sobre el resultado de la investigación reservada que, según el escrito formulado por esta entidad el día 16/01/2018 ante esta Autoridad, el ICS había iniciado en relación con los accesos llevados a cabo por Dª. . (...) en la historia clínica de la persona denunciante el día 27/03/2017; y aportara una copia de las actuaciones incorporadas al citado expediente informativo.

- Que el ICS Informara si la persona denunciante fue atendida como paciente en el CAP (...) en las fechas inmediatamente anteriores o posteriores al día 27/03/2017. Y en caso de que la persona denunciante no se hubiera visitado en ese centro sanitario, se indicaran los "motivos organizativos" que en el caso concreto explicarían los dos accesos controvertidos.
- Aportara una impresión de pantalla de los siguientes módulos de la ECAP correspondientes a la historia clínica de la persona denunciante:
  • "USUFG068-Etiquetas por Usuario"
  • "USUFG005-Mantenimiento de usuarios y pacientes".

Este acuerdo de prueba fue notificado el 04/10/2018 al ICS y se le otorgaba un plazo de 10 días para que diera cumplimiento a lo allí acordado.

9.- En fecha 29/10/2018 el ICS dio cumplimiento al acuerdo de prueba, y facilitó la siguiente información:

- Que "se ha visto que el acceso no era justificado".
- Que "se ha realizado información reservada sobre los accesos de Dª. (...). En este momento está en fase de investigación por parte del instructor, a fin de poder concluir y hacer propuesta de sanción, si es necesario"
- Que "La persona (denunciante) no fue visitada en el CAP (...), se han consultado las visitas pasadas de esta usuaria y no consta ninguna visita. Se desconocen los «motivos organizativos»"

Asimismo, el ICS aportó una impresión de pantalla del módulo "USUFG005-Mantenimiento de usuarios y pacientes".

10.- En fecha 05/11/2018, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos declarase que el ICS había incurrido en las siguientes infracciones:

10.1. En primer lugar, una infracción grave prevista en el artículo 44.3.d), en relación con el artículo 10 del LOPD.

10.2. En segundo lugar, una infracción grave prevista en el artículo 44.3.h), en relación con el artículo 9 del LOPD.

Esta propuesta de resolución se notificó en fecha 06/11/2018 y concedía un plazo de 10 días para formular alegaciones. Este plazo se ha superado y no se han presentado alegaciones.

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

Hechos probados

Del conjunto de las actuaciones practicadas en este procedimiento, se considerarán acreditados los hechos que se detallan a continuación.

1.- Una persona quien prestaba servicios como auxiliar administrativo en el CAP (...) –dependiente del Instituto Catalán de la Salud-, accedió el día 27/03/2017 en dos ocasiones a la historia clínica de la persona aquí denunciante (antecedente 1º), mediante la ECAP (programa informatizado de historias clínicas de atención primaria). Estos accesos se efectuaron sin que estuvieran justificados por ninguna actuación asistencial o administrativa.

2.- El Instituto Catalán de la Salud no revisa periódicamente la información de control registrada en el registro de accesos, ni elabora informes sobre las revisiones realizadas y los problemas detectados, sino que sólo se revisa a raíz de la petición concreta por parte de pacientes.

Fundamentos de derecho

1.- Son de aplicación a este procedimiento lo que prevén la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), y el artículo 15 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, 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.

Como consideración previa, cabe indicar que en el momento de dictarse este acto, el precepto que contenía el tipo infractor aquí aplicado se ha derogado por el Real decreto-ley 5/2018, de 27/7, de medidas urgentes para la adaptación del derecho español a la normativa de la Unión europea en materia de protección de datos. Pero al tratarse de un procedimiento sancionador iniciado antes de la vigencia de esta norma -o en el que las actuaciones previas que le habían precedido se habían iniciado antes-, debe regirse por la normativa anterior. (DT 1a RDL 5/2018).

Asimismo, en este acto se ha tenido en cuenta también la eventual aplicación en el caso presente de lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27/4, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de los mismos (RGPD). Y a resultas de este análisis se concluye que la eventual aplicación del RGPD no alteraría la calificación jurídica que aquí se hace, y en concreto no favorecería al presunto responsable de la infracción. En cualquier caso, cabe decir que los hechos imputados en aplicación de la LOPD también lo serían si se aplicara al caso el RGPD.

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

2.- La entidad imputada no ha formulado alegaciones a la propuesta de resolución, pero sí lo hizo en el acuerdo de iniciación. Al respecto, se considera oportuno reiterar a continuación el más relevante de la respuesta motivada de la persona instructora a estas alegaciones.

En su escrito de alegaciones en el acuerdo de iniciación, centradas únicamente en el primero de los hechos que aquí se declaran probados, relativo al acceso a la historia clínica, el ICS manifestaba que "en este caso no se ha producido vulneración alguna del deber de secreto ya que la señora (...) prestaba servicios como Auxiliar administrativa en el CAP (...) y en el ejercicio de sus funciones accedió a datos administrativos, no asistenciales, desde el ecap administrativo.
Entendemos que justificaron convenientemente el motivo del acceso y su justificación para la gestión de agendas, programación de visitas y otras tareas administrativas. El hecho de que sea un administrativo de un centro donde el paciente no tiene médico asignado se puede explicar por motivos organizativos, como alegamos, al ser de la propia Gerencia territorial".

Tal y como se ha recogido en los antecedentes, a la vista de las alegaciones formuladas, la instructora acordó la práctica de prueba para que el ICS aportara determinada información para esclarecer las circunstancias que en su caso habrían podido justificar los accesos imputados. Pues bien, en la práctica de la citada prueba el ICS admitió expresamente que estos accesos no estaban justificados,

Por otra parte, en el mismo escrito de alegaciones el ICS afirmaba que no se accedió a datos "asistenciales", sino únicamente a datos "administrativos". De esta imprecisa manifestación se podría inferir que el ICS viene a sostener que mediante los accesos controvertidos no se habría accedido a datos de salud, sino a datos únicamente administrativos. Pues bien, al respecto cabe decir que el tipo infractor que aquí se declara (vulneración del principio de confidencialidad) también se consumaría incluso en caso de que los módulos a los que accedió el auxiliar administrativo no contuvieran ningún dato relativo a la salud de la persona aquí denunciante.

3.- En relación con los hechos descritos en el punto primero del apartado de hechos probados, relativos al principio de confidencialidad, es necesario acudir al artículo 10 de la LOPD, que prevé lo siguiente:

> "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional en cuanto a los datos y al deber de guardarlos, obligaciones que subsisten incluso después de finalizar sus datos relaciones con el titular del fichero o, en su caso, con su responsable".

Tal y como indicaba la persona instructora, durante la tramitación de este procedimiento se ha acreditado debidamente que Dª. (...), auxiliar administrativa quien prestaría servicios en el CAP (...), a través de su código usuario que le permitía tener acceso al aplicativo ECAP, accedió a datos relativos a la persona denunciante contenidos en su historia clínica, sin que este acceso estuviera justificado por ninguna razón asistencial o administrativa. A este

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

respecto, cabe señalar que la legislación sanitaria, cuando regula los usos de la historia clínica, en lo referente a los profesionales sanitarios sólo contempla el acceso por parte de quienes asisten al paciente o que están implicados en su diagnóstico (art. 11 Ley 21 /2000 y 16 Ley 41/2002), circunstancia que no se daría aquí en los accesos referidos al apartado de hechos probados, los cuales por tanto vulneraban el principio de confidencialidad, actuación que a su vez se considera constitutiva de la infracción grave prevista en el artículo 44.3.d) de la LOPD, que tipifica como tal:

> "La vulneración del deber de guardar secreto sobre el tratamiento de los datos de carácter personal a que se refiere el artículo 10 de esta ley."

4.- En cuanto al hecho descrito en el punto 2 del apartado de hechos probados, respecto al cual el ICS no ha formulado ninguna alegación en sí de este procedimiento, es necesario acudir al artículo 9 del LOPD, que disponía lo siguiente:

> "El responsable del fichero y, en su caso, el encargado del tratamiento deben adoptar las medidas de carácter técnico y organizativo necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, el tratamiento o acceso no autorizado, teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos, tanto si proceden de la acción humana o del medio físico o natural."

Este desarrollo reglamentario en lo que se refiere a las medidas de seguridad a adoptar, se llevó a cabo mediante el RLOPD, y en concreto con su Título VIII. De acuerdo con el artículo 7.3 de la LOPD, los datos relativos a la salud eran datos especialmente protegidos, y como tales estaban sometidos a medidas de seguridad de nivel básico, medio y alto (art. 81.3.a RLOPD). Entre las medidas de nivel alto estaba la prevista en el apartado 5 del art. 103 del RLOPD referido a las obligaciones de control del responsable de seguridad, que en relación con el registro de accesos, estipula lo siguiente:

> "El responsable de seguridad debe encargarse de revisar al menos una vez al mes la información de control registrada y debe elaborar un informe de las revisiones realizadas y los problemas detectados".

Cabe decir que ante la entrada en vigor y plena aplicación del RGPD, y en particular de lo previsto en su art. 32 sobre la seguridad del tratamiento, el RLOPD no sería ya una norma directamente exigible, pero tal circunstancia no impide seguirlo considerando como una pauta o referencia válida en cuanto a la implementación de medidas que garanticen un nivel adecuado de seguridad en el tratamiento de los datos personales.

Además de lo anterior, también a modo de pauta o referencia se puede añadir que el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito del Administración electrónica, define el "registro de actividad" en su artículo 23:

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

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

El apartado 4.3.8 del Anexo II ("Medidas de Seguridad") del ENS, determina lo siguiente:

"Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información. b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadoras y administradoras en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema. c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados. d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista de la análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel BAJO Se activarán los registros de actividad en los servidores.
Nivel MEDIO Se revisarán informalmente los registros de actividad buscando patrones anormales.
Nivel ALTO Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada".

Y el Anexo 1 del ENS, relativo a "Categorías de los sistemas" determina que:

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:
1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sean desempeñándose. 2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.

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

3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Hay que añadir en relación con el ENS que el Centro Criptológico Nacional (del Estado Español) ha elaborado una "Guía de implantación del ENS" (actualizada en junio 2017) en qué punto 4.3.8 establece lo siguiente en relación con el "Registro de la actividad de los usuarios"

"225. Se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)
226. Se utilizan herramientas automáticas para recoger y analizar los registros en busca de actividades fuera de lo normal (por ejemplo: consola de seguridad centralizada, SIEM"

Esta Autoridad considera acreditado el hecho recogido en el punto 2º del apartado de hechos probados, lo que constituye una infracción grave del artículo 44.3.h) de la LOPD, que tipifica como tal:

"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que se determinen por vía reglamentaria."

5.- El artículo 21 de la Ley 32/2010, en consonancia con el artículo 46 de la LOPD, prevé que cuando las infracciones las comete una administración pública la resolución que declara la comisión de una infracción debe establecer las medidas que procede adoptar para que cesen o se corrijan sus efectos. En relación con esta cuestión, y tal y como expuso la instructora en la propuesta, cabe señalar lo siguiente:

5.1.- En cuanto al hecho probado 1º 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.

5.2.- En cuanto al hecho probado 2º, se requiere el ICS 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 esta resolución, implemente en el sistema de la ECAP 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 de la 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 los datos de los pacientes, con la elaboración del correspondiente informe, en la línea de lo que se había previsto en el art. 103.5 del RLOPD.

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

Una vez adoptada la medida correctora descrita en el plazo señalado, en el plazo de los 10 días siguientes el ICS debe informar a la Autoridad, sin perjuicio de la facultad de inspección de esta Autoridad para efectuar las verificaciones correspondientes.

5.3.- Por otra parte, cabe señalar que el artículo 21.2 de la Ley 32/2010, en consonancia con lo dispuesto en el artículo 46.2 de la LOPD, prevé la posibilidad de que la directora de la Autoridad proponga la iniciación de actuaciones disciplinarias, de acuerdo con lo que establece la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. En el caso aquí analizado esta Autoridad considera que no procede la proposición de actuaciones disciplinarias en la medida en que el ICS ha informado a esta Autoridad (antecedente 9º) que ha iniciado una información reservada en relación con los accesos injustificados que han dado origen a este procedimiento.

Resolución

Por todo esto, resuelvo:

1.- Declarar que el Instituto Catalán de la Salud ha cometido, en primer lugar, una infracción grave prevista en el artículo 44.3.d) en relación con el artículo 10; y en segundo lugar, una infracción grave prevista en el artículo 44.3.h), en relación con el artículo 9, todos ellos de la LOPD.

2.- Requerir el ICS para que adopte la medida correctora señalada en el fundamento de derecho 5º (apartado 2) y acredite ante esta Autoridad las actuaciones llevadas a cabo para cumplir con las mismas.

3.- Notificar esta resolución al Instituto Catalán de la Salud.

4.- Comunicar esta resolución al Síndic de Greuges y trasladarla literalmente, según lo especificado en el acuerdo tercero del Convenio de colaboración entre el Síndic de Greuges de Catalunya y la Agencia Catalana de Protección de Datos, de fecha 23 de junio de 2006.

5.- Ordenar que se publique esta resolución en la web de la Autoridad (www.apd.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.

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

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.

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

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

La directora

M. Àngels Barbarà y Fondevila

Barcelona, (a la fecha de la firma electrónica)