

Identificación del expediente

Resolución de archivo de la información previa núm. IP 452/2021, referente al Instituto Catalán de la Salud (Hospital Universitari Vall d'Hebron).

Antecedentes

1. En fecha 09/11/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de denuncia contra el Hospital Universitario Vall d'Hebron (HUVH), que depende del Instituto Catalán de la Salud (ICS), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

La persona denunciante exponía que había prestado servicios al HUVH como auxiliar administrativo y denunciaba las siguientes actuaciones que, a su entender, vulneraban la normativa de protección de datos:

- a) Que el personal del hospital con categoría de auxiliar administrativo puede acceder "de forma ilimitada, a cualquier dato personal y de salud de los pacientes del sistema de salud Autonómico Catalán", mediante el software "SAP" de gestión de historias clínicas del hospital.
- b) Que existe un equipo de auxiliares administrativos llamado "SIFCO", que se encarga de "gestionar y clasificar la revisión de las pruebas diagnósticas, así como las intervenciones y tratamientos realizados a pacientes de fuera de la Comunidad Autónoma Catalana", el cual no sólo tiene acceso a la integridad de la historia clínica, como el resto de auxiliares, sino que además "está encargado de clasificar dichas pruebas, tratamientos e intervenciones según la comunidad Autónoma y según el coste de las mismas."
- c) Que el personal auxiliar administrativo tiene un perfil que le permite "modificar la historia" clínica.
- d) Que el HUVH no forma adecuadamente a su personal en materia de protección de datos personales.
- e) Que el personal utiliza el correo corporativo como medio de "envío regular de, entre otros, correos electrónicos con capturas de imágenes del propio programa SAP."
- f) Que a dichos cuentas de correo electrónico se puede acceder desde cualquier dispositivo, teniendo únicamente un proceso de verificación primario de usuario y contraseña (siendo en todos los casos, el usuario el Número de Identificación Fiscal del trabajador).
- g) Que los profesionales del HUVH hacen uso de dispositivos "portables" "sin las salvaguardas ni medidas de seguridad necesarias para el cuidado de dicha información."
- h) Que el personal del hospital hace uso de la aplicación Whatsapp como medio de comunicación interno.

- i) Que hay m anca de medidas de seguridad en la atención a las personas usuarias, como por ejemplo “en la gestión de la información de los pacientes que a su ingreso solicitan no se entregue determinada información a “x” sujeto/s, (cómo sería el caso de violencia de género). Pues bien, puede observarse como una actividad cotidiana, como los trabajadores que ejercen sus funciones en puestos de atención al usuario, depositan el número de dicho paciente en un fragmento de papel, y lo depositan en la parte interna del mostrador.”
- j) Que no se ha definido correctamente el registro de actividades del tratamiento (RAT).
- k) Que no se ha realizado una evaluación de impacto correcta.

Con el fin de acreditar los hechos denunciados, la persona denunciante aportaba diversas impresiones de pantalla en las que constan los datos a los que habría podido acceder con su perfil de auxiliar administrativo. Entre otros:

- A. Impresiones en las que se observa que, mediante el software del hospital, la persona denunciante pudo acceder a la siguiente información relativa a su persona: a) curso clínico compartido, que incluye varias anotaciones detalladas sobre su estado de salud; yb) los resultados de determinados análisis.
- B. Impresiones en las que se observa que, a través del SAP, la persona denunciante pudo acceder a la denominación de las pruebas a las que se habrían sometido algunos pacientes.

2. La Autoridad abrió una fase de información previa (núm. IP 452/2021), 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 (LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador.

3. En fecha 25/11/2021, tuvo entrada un escrito de la persona denunciante por medio del cual ejercía su derecho de oposición ante esta Autoridad, en los siguientes términos:

“(…) interpuso una denuncia contra el Hospital Universitario Vall d'Hebron por varias brechas en la seguridad de las datos tratadas, tanto de sus trabajadores como de los pacientes de todo el Sistema de Salud Catalán. Debido a que me dedico al sector de la protección de datos en salud, el hecho de que se sepa la procedencia de la denuncia puede afectarme negativamente ya mis compañeros, por lo que me opongo a que el demandado sepa de mi identidad, con el fin de proteger al denunciante (…).”

4. En fecha 23/12/2021, la directora de la Autoridad dictó una resolución mediante la cual se estimó el derecho de oposición ejercido por la persona denunciante, en base a los motivos alegados en su solicitud de oposición.

5. En esta fase de información, en fecha 16/03/2022 se requirió la entidad denunciada para que informara, entre otras cuestiones:

- Se abre las categorías de profesionales que pueden acceder a la historia clínica hospitalaria y al HC3, a través del sistema de gestión de historias clínicas del HUVH (SAP);
- Sobre la información a la que puede acceder el personal con perfil de auxiliar administrativo (entre el que el equipo SIFCO), en relación con las funciones que tienen encomendadas;
- Sobre si el personal auxiliar administrativo puede modificar su historia clínica;
- sobre la formación en materia de protección de datos que el HUVH ofrece a su personal; sobre la utilización del correo corporativo, dispositivos portátiles y aplicación Whatsapp por parte del personal.
- Sobre la gestión de la información relativa a determinados pacientes (letra y antecedente 1º) por parte del personal de admisiones.

Por último, se la requirió para que aportara copia del Registro de actividades de tratamiento (RAT) y de la evaluación de impacto en materia de protección de datos (AIPD), en relación con las operaciones de tratamiento que se llevan a cabo en el 'HUVH.

6. En fecha 28/04/2022, la Autoridad reiteró el requerimiento de información señalado en el antecedente anterior.

7. En fecha 05/05/2022, el HUVH respondió a dicho requerimiento en los siguientes términos:

- Que a través del SAP se puede acceder al HC3 (base de datos de la que es responsable el Departamento de Salud), pero que sólo el personal colegiado tiene permitido el acceso. Por tanto, el personal con perfil de auxiliar administrativo no puede acceder.
- Que “en cuanto a la información que existe en el SAP, el personal del Hospital Universitario Vall d'Hebron accede según los perfiles existentes y establecidos desde el Centro Corporativo.”
- Que el perfil de auxiliar administrativo “no permite realizar modificaciones en la historia clínica. Los documentos que se incorporan al SAP, por parte de personal médico, quedan debidamente firmados y, en caso de producirse alguna modificación en algunos de estos documentos se guardan y quedan registradas las diferentes versiones, incluso en el caso de que se produzca una rayadura.”
- Que el departamento SIFCO (Sistema de Información del Fondo de Cohesión) “tiene una serie de peculiaridades debido a la necesidad de poder informar y justificar en el Ministerio de Sanidad, la actividad realizada al paciente de otra comunidad en nuestro hospital.” Que la gestión de la información que se genera a raíz de esta atención justifica que el personal administrativo acceda a información sanitaria de la persona usuaria (incluida en el HC hospitalaria -SAP-), a efectos de verificar si el paciente se encuentra dentro de un ensayo clínico, si es un usuario desplazado, si se han realizado pruebas determinadas, etc.
- Que el personal del HUVH se rige por la Instrucción 8/2020, de 24 de noviembre, sobre el uso de las tecnologías de la información y la comunicación en la

Administración de la Generalidad de Cataluña. Que todo el personal que se incorpora a trabajar en el HUVH debe firmar un documento titulado “Funciones y obligaciones de los usuarios y empleados”, en el que se exponen las normas de uso a respetar, en relación con las nuevas tecnologías de la información.

- Que el HUVH cuenta “con el apoyo y la creación de la “Comisión de Seguridad de Datos y RGPD”, cuya misión es “contribuir a la generación de una cultura de cumplimiento y respeto por los derechos y libertades fundamentales así como todos aquellos derechos y aspectos recogidos en el RPDG.” Que, a tal efecto, se programen cursos de formación para el personal en materia de protección de datos (se adjunta una relación de cursos efectuados y la presentación de cursos previstos para el año 2022).
- Que el RAT que se elabora "es a nivel de Centro Corporativo". Que, sin embargo, el HUVH dispone de un " SubRAT ", que se actualiza anualmente, donde se registran los tratamientos propios del Hospital.
- Que "la AIPD de SAP se elabora a nivel del Centro Corporativo."

La entidad denunciada adjuntaba, entre otra documentación, la siguiente:

- Documento titulado “ SubRAT ”, actualizado en el mes de diciembre de 2021.
- Documentación sobre AIPD relativa al software SAP.
- Documentación en relación con la gestión de la información de los pacientes que han solicitado la reserva de su identidad.

8. En fecha 27/05/2022, también en el seno de esta fase de información previa, se dirigió un oficio a la persona denunciante mediante el cual se le requería para que, en un plazo de 10 días, indicara si las tareas que desarrolla o desarrollaba en el HUVH se correspondían con las de un perfil administrativo con funciones de gestión del programa SIFCO.
9. En fecha 27/05/2022, en respuesta al oficio señalado en el antecedente anterior, la persona denunciante dirigió un escrito a la Autoridad en el que exponía que “Durante los tres años que trabajé en el Hospital VH, así como en otros centros del ICS, en jefe he llevado a cabo funciones con el programa SIFCO. En todo momento he ejecutado tareas de «auxiliar administrativo», a pesar de poder acceder a todo tipo de historiales y/o acciones dentro del curso clínico, dada la permeabilidad del programa SAP (en lo que se refiere a gestión de permisos) (.. .).”
10. En fecha 02/11/2022 y aún en el marco de esta fase de información previa, la Autoridad requirió nuevamente el HUVH para que ampliara alguna de la información facilitada en fecha 05/05/2022, en los términos que se planteaban al requerimiento de información señalado en el antecedente 5º. Asimismo, se le pidió explicaciones sobre el contenido de la información que aparecía en las impresiones de pantalla aportadas persona denunciante (letras A y B del antecedente 1º) que, según afirmaba, acreditaban que con su perfil de auxiliar administrativo había accedido a determinada información clínica [Hay que aclarar que en el requerimiento únicamente se hizo mención de forma genérica al contenido de estas impresiones, y no se proporcionó la copia de dichas

impresiones a la entidad denunciada, en la medida en que 'Autoridad estimó el derecho de oposición ejercido por la persona denunciante -antecedentes 3º y 4º-].

11. En fecha 02/03/2023 , la entidad denunciada amplió la respuesta que dio al requerimiento de la Autoridad de fecha 02/11/2022, en los siguientes términos:
- Que “el SAP Argos , tiene un sistema de perfiles de usuarios común a todos los Hospitales del Instituto Catalán de la Salud, es decir el Hospital de Vall Hebron cuando el Jefe de área responsable de gestionar los usuarios debe 'asignar un perfil a un nuevo trabajador debe seleccionar el perfil entre el listado de perfil predefinido en el propio aplicativo. No puede crear un perfil que no existe en el listado de SAP Argos . Este listado tiene aproximadamente unos 400 tipos de perfiles entre administrativos y asistenciales.” A modo de ejemplo, se aporta una impresión de pantalla "en la que se puede ver parte [30] de los diferentes perfiles que existen en el SAP de tipo administrativo."
 - Que “el mando superior (al ser la persona que conoce las funciones que va a desarrollar el nuevo trabajador) cuando se incorpora una persona al puesto de trabajo pide la creación de un nuevo usuario con un determinado perfil al Jefe de área responsable de la gestión de usuarios. Estos perfiles se crean en función del tipo de usuario (administrativo o asistencial) y del sitio o tipo de tarea que desarrolla (consultas externas, hospitalización, atención usuario...).”
 - Que, en lo que se refiere a las funcionalidades y acciones asignadas a cada perfil de usuario: “1. Como hemos indicado anteriormente, cada perfil tiene unos privilegios asignados, en función de la tarea que debe llevar a cabo, estas funcionalidades y acciones asignadas se pueden consultar en el SAP Argos por parte del jefe de unidad que crea los nuevos usuarios . Cada perfil de usuario tiene asignada una serie de acciones. (...) 2. Los diferentes perfiles administrativos pueden acceder a datos del SAP Argos que necesitan en función de la tarea que desarrollan, pueden modificar los datos de contacto del paciente (p.ex teléfono, dirección..), pero no pueden modificar datos sanitarios ni el curso clínico, es una funcionalidad reservada a los perfiles asistenciales.”
 - Que el HUVH “hace uso de la herramienta AUDIT de accesos a SAP, herramienta corporativa, a fin de establecer los mecanismos necesarios para dar cumplimiento a la normativa tanto en lo que se refiere a la revisión de accesos a las historias clínicas como en otros aspectos de carácter general relativos a la seguridad en el acceso a la información.”
 - Que, en relación con el acceso al HC3:
 - Este acceso “se regula por la Instrucción 06/2020 Implantación del encargo de gestión del Departamento de Salud en el Servicio Catalán de la Salud para que este último gestione la vinculación y el acceso a la historia clínica compartida (HC3) de los centros asistenciales integrados en el sistema sanitario integral de utilización pública de Cataluña (SISCAT) y otras entidades proveedoras del sistema público de salud». En esta instrucción se prevé que conforme a lo establecido en el artículo 11.1 de la Ley 21/2000 y el artículo 16.1 de la Ley

41/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, como instrumento fundamental para una adecuada asistencia.”

- “El alta en el HC3 se tramita por parte del propio Hospital pero siempre de acuerdo a lo establecido en la Instrucción que regula el uso del HC3, y con los requerimientos técnicos marcados por Departamento, que si no es introduce el número de colegiado del profesional sanitario, no se da acceso al HC3.”
 - “ El acceso al HC3 se hace a través del SAP Argos pero los profesionales de tipo administrativo no pueden acceder, ni por rol, ni porque técnicamente no tienen acceso al no tener número de colegiado.”
 - “Cuando un profesional se da de alta en el SAP Argos , si por su perfil también debe tener acceso al HC3 se le pide el número de colegiado y cuando accede al SAP Argos , tiene habilitado el acceso al SAP Argos HC3. (...) El acceso al SAP Argos no se da en función únicamente de la categoría laboral de la persona, sino en función de más elementos como las tareas que desarrolla o el puesto que ocupan (archivo, consultas externas, facturación. ..). Dicho esto, indicar que ningún perfil administrativo tiene «de forma ilimitada , a cualquier dato personal y de salud de los pacientes del sistema de salud Autonómico Catalán »”, tal y como manifestaba la persona denunciante.
 - “Los perfiles administrativos tienen acceso a los datos de los pacientes de Vall Hebron que necesitan para el desarrollo de sus funciones y no a los datos de pacientes de todo el sistema sanitario catalán. Entendemos que cuando el denunciante habla de datos de todo el sistema sanitario catalán se refiere al HC3, y este acceso sólo es posible con un número de colegiado, lo que por definición excluye cualquier rol administrativo que nunca tienen número de colegio. legiado. (...).”
- Que “en relación con las capturas de pantalla presentadas por la persona denunciante comentar que, dado que no disponemos de las capturas presentadas en la APDCAT, desconocemos a qué aplicación o sistema de información corresponden las capturas de pantalla mencionadas, si correspondían a captura de pantallas de su ordenador o de otro profesional, y en caso de estar el propio de trabajo de la persona denunciante, se desconoce el perfil de lo que disponía. Desconocemos a la persona de la que se trata, y el perfil de usuario que se le asignó por lo que no podemos describir qué privilegios exactos tenía, aunque como hemos comentado anteriormente, el perfil de administrativo sí puede acceder a datos del SAP Argos , no puede modificar los datos asistenciales ni puede acceder al HC3.”
- Que, en cuanto a la gestión del personal de admisiones de la información relativa a las personas que piden reserva sobre sus datos, cabe decir que “el programa de gestión SAP Argos dispone (...) de una funcionalidad en el SAP que puede anonimizar a un determinado paciente/usuario. Esta información se apoya en el documento nº 3 Manual de Usuario ARGOS, donde se detalla la funcionalidad de anonimización , entre otros, aportada en el primer escrito.”
- Que se reitera “que los profesionales del ICS se rigen por lo establecido en la Instrucción 8/2020 y, por tanto, se ponen a disposición del personal aquellas

herramientas necesarias para el cumplimiento de sus obligaciones de servicio y laborales. Asimismo, y de acuerdo con la citada Instrucción, los profesionales deben abstenerse de hacer un mal uso de las herramientas proporcionadas así como de la información no relacionada con las tareas y funciones encomendadas.”

- Que, en relación con la AIPD, y como información adicional a la ya aportada, se informa que “el ICS está llevando a cabo un procedimiento para coordinar a todos sus Hospitales en la realización de evaluaciones de impacto en base en la herramienta de AIPD creada por la Fundación TIC SALUD SOCIAL, específica para el sector salud, y que cuenta con un documento de procedimiento propio.”

Fundamentos de derecho

1. De acuerdo con lo que prevén los artículos 90.1 de la LPAC y 2 del Decreto 278/1993, en relación con el artículo 5 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el artículo 15 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, es competente para dictar esta resolución la directora de la Autoridad Catalana de Protección de Datos.
2. A partir del relato de antecedentes, se analizan los hechos denunciados que son objeto de esta resolución de archivo, de acuerdo con las consideraciones que se realizan en cada uno de los apartados:

2.1 Sobre la protección de datos por diseño y por defecto.

La persona denunciante manifestaba que el personal de la entidad denunciada, que ejerce funciones de auxiliar administrativo, puede acceder de forma "ilimitada" a las historias clínicas de los pacientes del sistema catalán de salud, y que puede modificar su contenido. Este hecho, de ser cierto, supondría que la definición de los perfiles profesionales efectuado por el HUVH para acceder al HC contravendría el artículo 25.1 del RGPD -que establece la obligación de proteger los datos personales desde el diseño, es decir, "tanto en el momento de determinar los medios de tratamiento, como en el momento del propio tratamiento"-, ya que estos profesionales podrían acceder a información que sería excesiva para ejercer sus funciones.

Lo primero que conviene poner de relieve es que, para acreditar este hecho denunciado, la única prueba que aportaba la persona denunciante, que afirmaba que había trabajado como auxiliar administrativo en el HUVH, era unas impresiones de pantalla en las que se podía visionar determinada información de asistencial y de salud (apartados A y B del antecedente 1º). Al respecto, cabe decir que, en fecha 25/11/2021, la persona denunciante ejerció su derecho de oposición ante la Autoridad y pidió explícitamente que no se comunicara su identidad como denunciante al HUVH, derecho que fue estimado mediante resolución de fecha 23/12/2021. Por este motivo, durante las actuaciones de inspección que se han llevado a cabo, no se ha podido consultar al HUVH sobre si el acceso a la información que consta en las impresiones de pantalla aportadas era necesario porque la persona denunciante desarrollara sus tareas. A este respecto, procede evidenciar que el ejercicio del derecho de oposición también ha impedido a la Autoridad trasladar las impresiones de pantalla a la entidad denunciada, para que pudiera contradecir o explicar la información que había aportado la persona denunciante.

Por su parte, el HUVH argumentó que el acceso a la información del SAP se configura a partir de un sistema de asignación de perfiles. Cada perfil tiene asociados determinados permisos, que le permiten visualizar los módulos de información autorizados. Esta herramienta dispone de aproximadamente cuatrocientos tipos de perfiles -entre personal administrativo (más de 30) y asistencial-, siendo el jefe de área responsable de la gestión de usuario quien se encarga de asignar los perfiles a los trabajadores que necesitan acceder a este sistema de información para desarrollar sus funciones.

En relación con lo anterior, la entidad denunciada añadía que la asignación de perfiles se lleva a cabo después de valorar si quien pide el acceso tiene un perfil administrativo o asistencial, y en atención a las tareas que la persona trabajadora tiene encomendadas (consultas externas, hospitalización, atención al usuario, entre otros). Al respecto, argumentaba que, en el ejercicio de determinadas funciones administrativas, algunos perfiles del SAP pueden modificar datos de contacto de las personas usuarias -por ejemplo, el teléfono o la dirección-, pero en cambio no pueden modificar ni las datos sanitarios, ni el curso clínico. En este sentido, sólo se autoriza el acceso a la información necesaria para desarrollar las funciones de un perfil profesional determinado.

De entre el personal administrativo con acceso "indiscriminado" a datos de salud, la persona denunciante destacaba aquél que presta servicio en el programa SIFCO, que, además de poder acceder a las historias clínicas de las personas usuarias del servicio, se encargaban de clasificar las pruebas, tratamientos e intervenciones de determinados pacientes.

Como cuestión previa, cabe tener presente que las siglas SIFCO obedecen al programa impulsado por el Ministerio de Sanidad, relativo al Sistema de Información del Fondo de Cohesión Sanitaria, regulado en el Real Decreto 1207/2006, de 20 de octubre. Este proyecto permite a los profesionales de salud derivar a un determinado paciente a un centro, servicio o unidad de referencia (CSUR) del Sistema Nacional de Salud.

Al respecto, el HUVH ha argumentado de forma suficiente que, con el objetivo de cumplir este programa, resulta necesario informar a las comunidades autónomas que lo necesitan, sobre las pruebas o tratamientos a las que se ha sometido un paciente determinado, para realizar el seguimiento médico que corresponda. Y, por estas razones, es necesario que haya un equipo de profesionales que se encargue de clasificar las pruebas, tratamientos e intervenciones (antecedente 7º).

En relación con lo anterior, hay que tener presente que el artículo 11.4 de la 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 prevé que, en relación con los usos de la historia clínica:

"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."

Asimismo, 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, regula en el artículo 16 los usos de la historia clínica, y prevé que el personal de

administración y gestión de los centros sólo pueda acceder a los datos de la historia clínica relacionados con sus funciones.

Por último, y en cuanto al acceso al HC3 (base de datos que depende del Departamento de Salud) por parte de las personas con perfil de auxiliar administrativo, la entidad denunciada ha expuesto que, a través del SAP, algunos perfiles también pueden acceder, pero que para ello es necesario informar previamente sobre el número de colegiación de la persona trabajadora. En consecuencia, dado que las personas que ocupan puestos de auxiliares administrativos no disponen de número de colegiación, cabe descartar que puedan acceder al HC3.

A la vista de lo que consta en las actuaciones y de acuerdo con lo expuesto, no se dispone de ningún elemento o indicio que permita sostener que las personas con perfil de auxiliar administrativo (incluido el personal del Departamento SIFCO) accedan a información excesiva en relación con las funciones que tienen encomendadas; tampoco que puedan modificar los datos clínicos de las personas usuarias del sistema de salud catalán.

2.3 Sobre la formación del personal

La persona denunciante manifestaba que el personal que presta servicios en el HUVH no recibe una formación adecuada en materia de protección de datos personales, señalando que tampoco se imparten formaciones periódicas en este ámbito.

Por su parte, el HUVH ha expuesto que, con el apoyo de la "Comisión de Seguridad de Datos y RGPD" de forma periódica se organizan cursos en materia de protección de datos dirigidos al personal de la entidad. A efectos de acreditarlo, ha aportado un extracto que permite constatar que, durante los años 2019 a 2021, se celebraron, como mínimo, 26 sesiones formativas, dirigidas a todo el personal.

En concordancia con el principio de responsabilidad proactiva, el responsable del tratamiento de datos debe adoptar todas las medidas técnicas y organizativas necesarias, incluida la formación a su personal, para poder demostrar que los tratamientos que realiza son conforme al RGPD. En este sentido, esta Autoridad no puede desconocer los esfuerzos del HUVH focalizados en concienciar y formar al personal que participa en las operaciones de tratamientos de datos personales, que han quedado suficientemente acreditados con la información aportada durante la fase de información previa.

2.4. Sobre el uso de herramientas de comunicación interna y dispositivos portables

2.4.1 Sobre el uso de herramientas de comunicación interna

La persona denunciante manifestaba que el personal del HUVH emplea la aplicación móvil "Whatsapp para la comunicación interna" y señalaba que el correo corporativo se utiliza para enviar de forma regular "mails electrónicos con capturas de imágenes del propio programa SAP. Esto no debería suponer un problema, siempre y cuando se regulasen correctamente las imágenes que son enviadas, así como la información suministrada, cosa que no es así."

Como cuestión previa, respecto del uso de la aplicación Whatsapp , cabe señalar que al considerante 18º y al artículo 2.2. c del RGPD se excluye el tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas . Tal y como se establece en el dictamen CNS 13/2018 de esta Autoridad, se entienden como actividades exclusivamente personales “ las que se inscriben en el marco de la vida privada o familiar de los particulares (art. 4. en RLOPD) o , como precisó la Audiencia Nacional en la Sentencia de 15 de junio de 2006: (...) Será personal cuando las datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos.”

Establecido lo anterior, aparte de las afirmaciones de la persona denunciante, esta Autoridad no dispone de ningún elemento que permita inferir que el personal del HUVH emplea dicha aplicación para efectuar comunicaciones corporativas.

Por otra parte, en relación con el uso del correo corporativo, la persona denunciante afirmaba que “ los trabajadores utilizan el correo corporativo sin filtro a la hora de enviar información personal de los afectados, sin calcular que dichos correos electrónicos, con dicha información , pueden ser enviados a correos electrónicos ajenos al Hospital; y que a dichos cuentas de correo electrónico se puede acceder desde cualquier dispositivo (...)”.

Al respecto, no cabe duda de que la herramienta del correo electrónico corporativo constituye un instrumento de comunicación y gestión básico e imprescindible en muchas organizaciones, y que su uso indebido puede poner en riesgo la seguridad de los datos.

Por su parte, el HUVH ha informado que su personal se rige por lo que establece la Instrucción 8/2020 y que, de acuerdo con esta norma, los profesionales deben abstenerse de hacer un mal uso de las herramientas proporcionadas, así como de la información no relacionada con las tareas y funciones encomendadas; y que todo el personal que se incorpora a trabajar en el HUVH debe firmar un documento titulado Funciones y obligaciones de los usuarios y empleados, en el que se exponen las normas de uso a respetar, en relación con las nuevas tecnologías de la información.

También hay que decir que el acceso a la cuenta de correo corporativo, que según manifestaba el denunciante podía hacerse desde cualquier dispositivo, en sí mismo no supone una vulneración de la normativa de protección de datos -y específicamente de ninguna medida de seguridad-, ya que para acceder es necesario acreditarse mediante usuario y contraseña. Eso sí, la persona trabajadora debe evitar que terceras personas puedan acceder a la información relacionada con su puesto de trabajo que se intercambie a través de este medio. Y en este punto conviene recordar que, de conformidad con el artículo 11.6 de la Ley 21/2000, de 29 de diciembre, el personal que accede a información de la historia clínica en el ejercicio de sus funciones está sujeto al deber de guardar secreto. Este deber también está previsto en el artículo 16.6 de la Ley 41/2002, de 14 de noviembre.

En definitiva, aparte de las manifestaciones de la persona denunciante, no consta acreditado que mediante el correo electrónico corporativo o de la aplicación Whatsapp , el personal del HUVH haya filtrado información de los pacientes o personas trabajadoras del centro y haya contravenido, así, el RGPD.

2.4.2 Sobre el uso de dispositivos portables

Tal y como se desprende de los antecedentes, el escrito de denuncia también tiene por objeto poner de manifiesto que el personal del HUVH emplea dispositivos portables "sin las salvaguardas ni medidas de seguridad necesarias."

Al respecto, la persona denunciante no concreta qué dispositivos portables incumplirían la normativa de protección de datos (ordenadores, tabletas o móviles, entre otros), ni si se refiere a dispositivos de tipo personal o profesional. Además, tampoco señala los motivos por los que considera que se vulnera la obligación de adoptar medidas de seguridad adecuadas (art. 25 y 32 RGPD).

2.5. Sobre el RAT y el AIPD

La persona denunciante manifestaba que el HUVH no habría definido correctamente ni el RAT, ni el AIPD, dado que, según argumenta, no se habría tenido en cuenta el ámbito en el que se tratan los datos personales, ni se habrían implementado las medidas de seguridad aplicables.

Es necesario señalar que el ICS es la entidad encargada de gestionar el HUVH y ejerce la condición de responsable del tratamiento de los datos personales que lleva a cabo la entidad denunciada.

Una vez establecido lo anterior, el artículo 30 del RGPD dispone que cada responsable del tratamiento –en este caso, el ICS– debe disponer de un registro de las actividades de tratamiento que lleva a cabo, y lo prevé el contenido mínimo.

La entidad denunciada ha aportado a la Autoridad el RAT elaborado por el ICS, así como un documento titulado SubRAT, que se actualiza anualmente. Este documento recoge los tratamientos de datos personales que realiza el hospital denunciado, así como los perfiles profesionales que tienen acceso a la información.

El HUVH también ha aportado la AIPD elaborada en relación con el tratamiento de datos personales vinculado al SAP, que también recoge los puntos previstos en el artículo 35 RGPD sobre el contenido de las evaluaciones de impacto relativas a la protección de datos. Tanto el ICS -como responsable del tratamiento-, como el HUVH han tratado datos personales desde antes de la entrada en vigor de RGPD; este hecho es especialmente relevante dado que, de acuerdo con el criterio de las autoridades de control, cuando los tratamientos de datos se han iniciado antes de la entrada en vigor del RGPD sólo es obligatorio llevar a cabo una AIPD si se producen cambios sustanciales que afecten al tratamiento.

3. El artículo 10.2 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, prevé que "(...) no se formulará pliego de cargos y se ordenará el sobreseimiento del expediente y el archivo de las actuaciones cuando de las diligencias y de las pruebas practicadas, resulte acreditada la inexistencia de infracción o responsabilidad. Esta resolución se

notificará a los interesados”. Y el artículo 20.1) del mismo Decreto determina que procede el sobreseimiento: “a) Cuando los hechos no son constitutivos de infracción administrativa; b) Cuando no existen indicios racionales de haberse producido los hechos que han sido la causa de la iniciación del procedimiento.”

De conformidad con todo lo expuesto en el fundamento de derecho 2º y dado que durante las actuaciones llevadas a cabo en el marco de la información previa no se ha acreditado, en relación con los hechos que se han abordado en la misma resolución, ningún hecho que pueda ser constitutivo de alguna de las infracciones previstas en la legislación sobre protección de datos, procede acordar su archivo.

Resolución

Por tanto, resuelvo:

1. Archivar las actuaciones de información previa número IP 452/2021, relativas al Instituto Catalán de la Salud (Hospital Universitario Vall d'Hebron), dado que durante las actuaciones llevadas a cabo en el marco de la información previa no se ha constatado que se haya producido ningún acto que pueda ser constitutivo de alguna de las infracciones previstas en la legislación sobre protección de datos.
2. Notificar esta resolución al Instituto Catalán de la Salud (Hospital Universitari Vall d'Hebron) y comunicarla a la persona denunciante.
3. Ordenar que esta resolución se publique 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 el artículo 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, el entidad denunciada 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 al de su notificación, de acuerdo con el que prevé el artículo 123 y siguientes de la Ley 39/2015. También se 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.

Asimismo, las personas interesadas pueden interponer cualquier otro recurso que considere conveniente para defender sus intereses.

La directora