apdcat
Autoritat Catalana de Protecció de Dades

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

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 14/2020, referente a la Corporación Sanitaria Parc Taulí.

Antecedentes

1. En fecha 17/05/2019, tuvo entrada en la Autoridad Catalana de Protección de Datos, por remisión de la Oficina Antifraude de Cataluña, un escrito en el que se indicaba que se podía acceder a los más de "3.000 ordenadores de sobremesa [que] se utilizan en el Hospital Universitario Parc Taulí de Sabadell", a través de un mismo código de usuario ("CSPT") y contraseña ((...)).

2. La Autoridad abrió una fase de información previa (núm. IP 153/2019), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

3. En esta fase de información, en fecha 09/07/2019, la Autoridad llevó a cabo un acto de inspección en las dependencias del Hospital de Sabadell de la Corporación Sanitaria Parc Taulí (en adelante, CSPT) , para verificar determinados aspectos relacionados con los hechos. En ese acto de inspección presencial, los representantes de la CSPT manifestaron lo siguiente:

ÿ Que las personas empleadas de la CSPT, para iniciar la sesión informática a través de los ordenadores de sobremesa, debían identificarse a través de un código de usuario y autenticarse mediante una contraseña.
ÿ Que había usuarios que compartían código de usuario y contraseña. Estos códigos de usuario genéricos se utilizaban para acceder a las unidades locales de los ordenadores. Para acceder a sus datos personales (carpetas, aplicaciones, unidades de red, etc.), cada persona tenía su código de usuario personal.
ÿ Que los códigos de usuarios genéricos eran "CSPT", "consultas", "enfermería" y "UDIAT".
ÿ Que en principio, no se almacenaban datos personales en el disco duro local de estos ordenadores. Las personas usuarias disponían de unidades de red que eran personales y también de grupo (por cada unidad), para almacenar archivos con datos personales.
ÿ Que en la guía corporativa de confidencialidad, se indicaba de forma genérica que no se podía almacenar información con datos personales en los discos duros locales.
ÿ Que se hizo una acción para que, las personas usuarias que lo justificaran, pudieran disponer de más espacio en las unidades de red personales y de grupo.
ÿ Que para acceder a las aplicaciones que utilizaban las personas usuarias (como la que permitía consultar la historia clínica), era necesario identificarse y autenticarse nuevamente. El código de usuario y contraseña era diferente para cada usuario.

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

ÿ Que para acceder a las unidades de red también se disponía de usuario y contraseña personal.
ÿ Que en marzo de 2019 aproximadamente, se deshabilitó la posibilidad de acceder o conectarse al disco duro de cualquier otro ordenador de la red informática.
ÿ Que estaba previsto efectuar un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos que trata la CSPT a través de la red informática.

Asimismo, en esa misma fecha, el personal inspector de la Autoridad verificó, entre otros, lo siguiente:

ÿ Que para iniciar la sesión informática del equipo informático de la unidad de programación de visitas, el código de usuario era "CSPT" y la contraseña era (...).
ÿ Que en la carpeta "Documentos" de la unidad local de aquel equipo informático había ficheros que contenían datos personales, entre ellos referentes a la salud.
ÿ Que, para acceder a la aplicación para consultar la historia clínica de los pacientes (HP-HCIS TAULI), el código de usuario era personal.
ÿ Que para acceder a las unidades de red era necesario identificarse y autenticarse previamente. El código de usuario también era personal.
ÿ Que no se podía acceder remotamente al disco duro de otro ordenador.

4. En fecha 02/06/2020, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra la CSPT por dos presuntas infracciones, en ambos casos, previstas en el artículo 83.4.a), en relación en el artículo 32; todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD).

5. En fecha 26/06/2020, la CSPT formuló alegaciones al acuerdo de iniciación.

6. En fecha 15/09/2020, 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 amonestara a la CSPT como responsable de dos infracciones previstas en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 25/09/2020.

7. En fecha 08/10/2020, la entidad imputada ha presentado un escrito por el que manifiesta que no formula alegaciones a la propuesta de resolución, y simplemente informa sobre las actuaciones llevadas a cabo para dar cumplimiento a las medidas correctoras que proponía a la persona instructora.

A su vez, la CSPT aportaba copia del análisis de riesgos sobre la seguridad de las estaciones de trabajo.

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

Hechos probados

1. Según informaron los representantes de la CSPT en el acto de inspección presencial efectuado el 09/07/2019 por personal inspector de la Autoridad, para iniciar la sesión informática a través de los ordenadores de sobremesa, las personas usuarias debían identificarse a través de un código de usuario genérico ("CSPT", "consultas", "enfermería" o "UDIAT") y autenticarse mediante una contraseña que era común para cada código de usuario genérico.

Tal y como constató el personal inspector de la Autoridad en el mismo acto de inspección, una vez iniciada la sesión informática de la unidad de programación de visitas con el código de usuario "CSPT" y la contraseña (...), en la unidad local de ese equipo se almacenaban documentos con datos personales relativos a la salud de pacientes de la CSPT.

A su vez, y según admitieron los representantes de la CSPT en el mismo acto de inspección, hasta aproximadamente el mes de marzo de 2019, una vez iniciada la sesión informática en ordenador de la CSPT mediante un código de usuario genérico , existía la posibilidad de acceder o conectarse al disco duro de cualquier otro ordenador de la red informática.

El personal inspector de la Autoridad, verificó en el acto de inspección que ya no podía accederse remotamente al disco duro de otro ordenador.

2. Tal y como admitieron también los representantes de la CSPT en el acto de inspección, no se había efectuado un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos que trataba la CSPT a través de la red informática.

Fundamentos de derecho

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

2. Tal y como se ha avanzado en los antecedentes, la CSPT 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 lo más relevante de la respuesta motivada de la persona instructora a estas alegaciones.

2.1. Sobre el hecho probado 1r.

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

En primer lugar, la entidad imputada remarcaba en su escrito de alegaciones ante el acuerdo de iniciación, que la disposición de carpetas personales en unidades de red (que requieren de una contraseña), aseguraba la posibilidad de almacenar datos personales con las medidas de seguridad de acuerdo con la normativa vigente. Y añadía que los datos personales compartidos en estas carpetas estaban justificados por necesidad de la atención que se presta en la CSPT.

En relación a lo anterior, tal y como indicaba la persona instructora en la propuesta de resolución, es necesario puntualizar que ninguna de las dos circunstancias que exponía la CSPT son objeto de imputación en el presente procedimiento sancionador.

En segundo lugar, la CSPT admitía que algunos usuarios, como se evidenció en la inspección llevada a cabo por el personal inspector de la Autoridad, conservaban en el disco duro datos personales que deberían almacenarse en dichas unidades de red. Por ello, la CSPT consideraba que esta incidencia debía circunscribirse al acceso a los datos del disco local de los ordenadores sin clave de paso personalizada.

En efecto, tal y como se expone en el 1er punto del apartado de hechos probados, el personal inspector de la Autoridad constató que una vez iniciada la sesión informativa identificándose con uno de los códigos de usuarios genéricos que empleaba la CSPT, y autenticándose con una contraseña común, se podía acceder a documentos con datos personales relativos a la salud de pacientes de la CSPT que se conservaban en la unidad local de un determinado equipo informático.

Por el contrario, tal y como se recoge en el antecedente 3º, en el acto de inspección presencial el personal inspector de la Autoridad verificó que para acceder a la aplicación para consultar la historia clínica de los pacientes o en las unidades de red, el código de usuario era personal.

Y, en tercer lugar, la CSPT argumentaba que en las auditorías realizadas (la última, en 2017) no se detectó las incidencias a que se refiere el hecho probado 1º de esta propuesta.

Pues bien, el hecho de que en las auditorías sobre protección de datos que llevó a cabo la CSPT no se detectaran los hechos objeto de imputación, no permiten eximir de responsabilidad a la CSPT.

2.2. Acerca de las medidas correctoras.

Seguidamente, la entidad imputada aducía en su escrito de alegaciones ante el acuerdo de iniciación que se había previsto la supresión de los usuarios genéricos, pero exponía que la complejidad del proyecto, el coste y la situación derivada del estado de alarma, la habían demorado.
Sin embargo, la CSPT señalaba que había reanudado el proyecto, que se había redefinido por fases.

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

Mientras no se ejecuta dicho proyecto, y para garantizar que no se puedan almacenar datos sin necesidad de autenticarse, la CSPT manifestaba que se había ampliado el espacio dedicado a los archivos de los usuarios, el cual siempre requería la autenticación mediante contraseña personal.

Asimismo, la CSPT indicaba que a través de la intranet se había comunicado a todos los empleados que no se podían guardar archivos que contuvieran datos personales en el disco duro del ordenador, al no garantizar la seguridad de los datos; que no se podía guardar información con datos personales fuera de las bases de datos corporativas (y que en caso de ser imprescindible, que se utilizaran las carpetas de la red); así como que se había ampliado el espacio de almacenamiento de que disponían los usuarios. Con similar contenido, la CSPT envió un mensaje a todos los empleados mediante una ventana emergente y configuró otro mensaje que se mostraba en el momento de puesta en funcionamiento del equipo informático.

Por otra parte, la CSPT también enumeraba una serie de medidas que, a su criterio, evidenciaban su responsabilidad proactiva (la adhesión a un determinado código tipo, la realización de auditorías bienales, el acceso por parte de los empleados a la guía para el cuidado de la confidencialidad, la difusión de novedades sobre protección de datos a través de la intranet, la realización de auditorías mensuales de registro de accesos, la realización de actividades formativas sobre protección de datos, el nombramiento de un delegado de protección de datos o la realización de distintos procedimientos internos).

Al respecto, cabe decir que las circunstancias invocadas por la CSPT para acreditar su responsabilidad proactiva, se podrían tener en cuenta para graduar la cuantía económica de la sanción en caso de que ésta consistiera en la imposición de una multa administrativa, de conformidad con lo establecido en el artículo 83.4 del RGPD.

Ahora bien, en el presente caso el régimen sancionador aplicable a la CSPT no prevé la imposición de una sanción económica, sino la amonestación de acuerdo con lo previsto en el artículo 77 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), que por su propia naturaleza no es susceptible de graduación.

Sin embargo, tal y como señalaba la persona instructora, corresponde destacar y valorar las medidas de responsabilidad proactiva adoptadas por la entidad imputada y las que tenía previsto implementar a raíz de los hechos objeto del presente procedimiento sancionador, las cuales deben permitir (cuando estén plenamente implementadas) corregir los efectos de la infracción vinculada al hecho probado 1º (el uso de códigos de usuario y contraseñas genéricos para iniciar la sesión informática a través de los ordenadores de sobremesa, lo que permitía acceder a la unidad local del equipo en la que se almacenaban documentos con datos personales, así como la posibilidad de acceder remotamente al disco duro de otro ordenador de la red de la CSPT (lo que se enmendó durante el mes de marzo de 2019, aproximadamente-).

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

Por último, la CSPT también detallaba de forma extensa una serie de acciones que se realizaron para incrementar la seguridad de los datos, fruto del informe de análisis de riesgos.

Pues bien, en la propuesta de resolución se valoraba positivamente la realización de dicho análisis de riesgos por parte de la CSPT (si bien éste no se había aportado).

Dicho esto, tal y como exponía la persona instructora, también es necesario puntualizar que la adopción de medidas para corregir los efectos de la infracción no desvirtúan los hechos imputados, ni tampoco modifican su calificación jurídica.

3. En relación con las dos conductas descritas en el apartado de hechos probados, es necesario acudir al artículo 5.1.f) del RGPD, que regula el principio de integridad y confidencialidad determinado que los datos personales serán "tratados de tal forma que se garantice una seguridad adecuada de las datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".

Por su parte, el artículo 32.1 del RGPD prevé que "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y las fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (...)."

A su vez, el artículo 32.2 del RGPD dispone que "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."

Esto implica tener que realizar una evaluación de los riesgos que comporta cada tratamiento, para determinar las medidas de seguridad a implementar.

Sin perjuicio de dicha evaluación, el apartado 2º de la disposición adicional 1ª de la LOPDDDD establece que "Los responsables que enumera el artículo 77.1 de esta Ley orgánica deben aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las que prevé el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones sujetas al derecho privado vinculadas a aquéllos."

En este sentido, el artículo 16 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, contempla como uno de los requisitos mínimos de seguridad en lo referente a la autorización y control de los accesos, que "El acceso al sistema de información deberá ser controlado y limitado a los

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

usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas."

Sin embargo, en el presente caso el uso de un sistema de identificación y autenticación genérico para iniciar la sesión en los equipos informáticos, no garantizaba el control de los accesos.

Tal como indicaba la persona instructora, durante la tramitación de este procedimiento se han acreditado debidamente las dos conductas descritas en el apartado de hechos probados, que son constitutivas de dos infracciones, ambas previstas en el artículo 83.4.a) el 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 prevista en el artículo 32 RGPD.

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. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente:

> "(...) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.
>
> La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso."

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010, determina lo siguiente:

> "2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos . Además, puede proponer, en su caso, 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. Esta resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan ya las personas afectadas, si las hubiere".

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

Tal y como se ha avanzado en los antecedentes, mediante escrito de 08/10/2020 la CSPT ha aportado copia del análisis de riesgos sobre la seguridad de las estaciones de trabajo, por lo que no corresponde requerir ninguna medida correctora en relación con el hecho probado 2º.

Por otra parte, en relación a la medida correctora que proponía la persona instructora en la propuesta de resolución en lo que se refiere al hecho probado 1º, la CSPT informa en su escrito de 08/10/2020 que se han iniciado las acciones correctoras oportunas para darle respuesta en el plazo señalado en la propuesta de resolución, lo cual se debe valorar positivamente.

Dado lo anterior, procede requerir a la CSPT para que lo antes posible, y en todo caso en el plazo máximo de 3 meses a contar desde el día siguiente de la notificación de esta resolución, lleve a cabo las actuaciones necesarias para garantizar la identificación y autenticación personalizada de los usuarios autorizados para acceder a los equipos informáticos; suprimiendo los usuarios genéricos ahora existentes.

Una vez adoptada la medida correctora descrita, en el plazo señalado, es necesario que en los 10 días siguientes la CSPT informe a la Autoridad, sin perjuicio de la facultad de inspección de esta Autoridad para realizar las verificaciones correspondientes.

Resolución

Por todo esto, resuelvo:

1. Amonestar a la Corporación Sanitaria Parc Taulí como responsable de dos infracciones previstas en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

2. Requerir a la CSPT para que adopte la medida correctora señalada en el fundamento de derecho 4º y acredite ante esta Autoridad las actuaciones llevadas a cabo para cumplirla.

3. Notificar esta resolución a la CSPT.

4. Comunicar la resolución que se dicte en el Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 de la LOPDDDD.

5. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos 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

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

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,