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

## Identificació de l'expedient

Resolució del procediment sancionador núm. PS 14/2020, referent a la Corporació Sanitària Parc Taulí.

## Antecedents

1. En data 17/05/2019, va tenir entrada a l'Autoritat Catalana de Protecció de Dades, per remissió de l'Oficina Antifrau de Catalunya, un escrit en què s'indicava que es podia accedir als més de *"3.000 ordinadors de sobretaula* [que] *es fan servir a l'Hospital Universitari Parc Taulí de Sabadell"*, a través d'un mateix codi d'usuari (*"CSPT"*) i contrasenya (*(...)*).

2. L'Autoritat va obrir una fase d'informació prèvia (núm. IP 153/2019), d'acord amb el que preveu l'article 7 del Decret 278/1993, de 9 de novembre, sobre el procediment sancionador d'aplicació als àmbits de competència de la Generalitat, i l'article 55.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (d'ara endavant, LPAC), per determinar si els fets eren susceptibles de motivar la incoació d'un procediment sancionador, la identificació de la persona o persones que en poguessin ser responsables i les circumstàncies rellevants que hi concorrien.

3. En aquesta fase d'informació, en data 09/07/2019, l'Autoritat va dur a terme un acte d'inspecció a les dependències de l'Hospital de Sabadell de la Corporació Sanitària Parc Taulí (en endavant, CSPT), per verificar determinats aspectes relacionats amb els fets. En aquell acte d'inspecció presencial, els representants de la CSPT van manifestar el següent:

- Que les persones empleades de la CSPT, per iniciar la sessió informàtica a través dels ordinadors de sobretaula, havien d'identificar-se a través d'un codi d'usuari i autenticar-se mitjançant una contrasenya.
- Que hi havia usuaris que compartien codi d'usuari i contrasenya. Aquests codis d'usuari genèrics s'utilitzaven per accedir a les unitats locals dels ordinadors. Per accedir a les dades personals (carpetes, aplicacions, unitats de xarxa, etc.), cada persona tenia el seu codi d'usuari personal.
- Que els codis d'usuaris genèrics eren *"CSPT", "consultes", "infermeria"* i *"UDIAT"*.
- Que en principi, no s'emmagatzemaven dades personals en el disc dur local d'aquest ordinadors. Les persones usuàries disposaven d'unitats de xarxa que eren personals i també de grup (per cada unitat), per emmagatzemar fitxers amb dades personals.
- Que en la guia corporativa de confidencialitat, s'indicava de forma genèrica que no es podia emmagatzemar informació amb dades personals en els discs durs locals.
- Que es va fer una acció per tal que, les persones usuàries que ho justifiquessin, poguessin disposar de més espai en les unitats de xarxa personals i de grup.
- Que per accedir a les aplicacions que utilitzaven les persones usuàries (com ara la que permetia consultar la història clínica), calia identificar-se i autenticar-se novament. El codi d'usuari i contrasenya era diferent per a cada persona usuària.

– Que per accedir a les unitats de xarxa també es disposava d'usuari i contrasenya personal.
– Que el març de 2019 aproximadament, es va deshabilitar la possibilitat d'accedir o connectar-se al disc dur de qualsevol altre ordinador de la xarxa informàtica.
– Que estava previst efectuar una anàlisi de riscos per determinar les mesures tècniques i organitzatives apropiades per garantir la seguretat de les dades que tracta la CSPT a través de la xarxa informàtica.

Així mateix, en aquesta mateixa data, el personal inspector de l'Autoritat va verificar, entre d'altres, el següent:

– Que per iniciar la sessió informàtica de l'equip informàtic de la unitat de programació de visites, el codi d'usuari era *"CSPT"* i la contrasenya era *(...)*.
– Que en la carpeta *"Documents"* de la unitat local d'aquell equip informàtic hi havia fitxers que contenien dades personals, entre les quals de referents a la salut.
– Que, per accedir a l'aplicació per consultar la història clínica dels pacients (HP-HCIS TAULI), el codi d'usuari era personal.
– Que per accedir a les unitats de xarxa calia identificar-se i autenticar-se prèviament. El codi d'usuari també era personal.
– Que no es podia accedir remotament al disc dur d'un altre ordinador.

4. En data 02/06/2020, la directora de l'Autoritat Catalana de Protecció de Dades va acordar iniciar un procediment sancionador contra la CSPT per dues presumptes infraccions, en ambdós casos, previstes a l'article 83.4.a), en relació a l'article 32; tots ells del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes (en endavant, RGPD).

5. En data 26/06/2020, la CSPT va formular al·legacions a l'acord d'iniciació.

6. En data 15/09/2020, la persona instructora d'aquest procediment va formular una proposta de resolució, per la qual proposava que la directora de l'Autoritat Catalana de Protecció de Dades amonestés la CSPT com a responsable de dues infraccions previstes a l'article 83.4.a) en relació amb l'article 32, ambdós de l'RGPD.

Aquesta proposta de resolució es va notificar en data 25/09/2020.

7. En data 08/10/2020, l'entitat imputada ha presentat un escrit pel qual manifesta que no formula al·legacions a la proposta de resolució, i simplement informa sobre les actuacions dutes a terme per donar compliment a les mesures correctores que proposava la persona instructora.

Al seu torn, la CSPT aportava còpia de l'anàlisi de riscos sobre la seguretat de les estacions de treball.

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

## Fets provats

1. Segons van informar els representants de la CSPT en l'acte d'inspecció presencial efectuat el 09/07/2019 per personal inspector de l'Autoritat, per iniciar la sessió informàtica a través dels ordinadors de sobretaula, les persones usuàries havien d'identificar-se a través d'un codi d'usuari genèric (*"CSPT", "consultes", "infermeria"* o *"UDIAT"*) i autenticar-se mitjançant una contrasenya que era comuna per a cada codi d'usuari genèric.

Tal com va constatar el personal inspector de l'Autoritat en el mateix acte d'inspecció, un cop iniciada la sessió informàtica de la unitat de programació de visites amb el codi d'usuari *"CSPT"* i la contrasenya *(...)*, en la unitat local d'aquell equip s'emmagatzemaven documents amb dades personals relatives a la salut de pacients de la CSPT.

Al seu torn, i segons van admetre els representats de la CSPT en el mateix acte d'inspecció, fins aproximadament el mes de març de 2019, un cop s'iniciava la sessió informàtica en ordinador de la CSPT mitjançant un codi d'usuari genèric, hi havia la possibilitat d'accedir o connectar-se al disc dur de qualsevol altre ordinador de la xarxa informàtica.

El personal inspector de l'Autoritat, verificà en l'acte d'inspecció que ja no es podia accedir remotament al disc dur d'un altre ordinador.

2. Tal com van admetre també els representants de la CSPT en l'acte d'inspecció, no s'havia efectuat una anàlisi de riscos per determinar les mesures tècniques i organitzatives apropiades per garantir la seguretat de les dades que tractava la CSPT a través de la xarxa informàtica.

## Fonaments de dret

1. Són d'aplicació a aquest procediment el que preveuen l'LPAC, i l'article 15 del Decret 278/1993, segons el que preveu la DT 2a de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades. De conformitat amb els articles 5 i 8 de la Llei 32/2010, la resolució del procediment sancionador correspon a la directora de l'Autoritat Catalana de Protecció de Dades.

2. Tal com s'ha avançat en els antecedents, la CSPT no ha formulat al·legacions a la proposta de resolució, però sí que ho va fer a l'acord d'iniciació. Respecte d'això, es considera oportú reiterar a continuació el més rellevant de la resposta motivada de la persona instructora a aquestes al·legacions.

2.1. Sobre el fet provat 1r.

En primer lloc, l'entitat imputada remarcava en el seu escrit d'al·legacions davant l'acord d'iniciació, que la disposició de carpetes personals en unitats de xarxa (les qual requereixen d'una contrasenya), assegurava la possibilitat d'emmagatzemar dades personals amb les mesures de seguretat d'acord amb la normativa vigent. I afegia que les dades personals compartides en aquestes carpetes estaven justificades per necessitat de l'atenció que es presta a la CSPT.

En relació a l'anterior, tal com indicava la persona instructora en la proposta de resolució, és necessari puntualitzar que cap de les dues circumstàncies que exposava la CSPT són objecte d'imputació en el present procediment sancionador.

En segon lloc, la CSPT admetia que alguns usuaris, com es va evidenciar en la inspecció duta a terme pel personal inspector de l'Autoritat, conservaven en el disc dur dades personals que haurien d'emmagatzemar-se en les unitats de xarxa esmentades. És per això, que la CSPT considerava que aquesta incidència calia circumscriure-la a l'accés a les dades del disc local dels ordinadors sense clau de pas personalitzada.

En efecte, tal com s'exposa en el 1r punt de l'apartat de fets provats, el personal inspector de l'Autoritat va constatar que un cop iniciada la sessió informativa identificant-se amb un dels codis d'usuaris genèrics que emprava la CSPT, i autenticant-se amb una contrasenya comuna, es podia accedir a documents amb dades personals relatives a la salut de pacients de la CSPT que es conservaven en la unitat local d'un determinat equip informàtic.

Per contra, tal com es recull en l'antecedent 3r, en l'acte d'inspecció presencial el personal inspector de l'Autoritat va verificar que per accedir a l'aplicació per consultar la història clínica dels pacients o a les unitats de xarxa, el codi d'usuari era personal.

I, en tercer lloc, la CSPT argumentava que en les auditories realitzades (la darrera, l'any 2017) no es va detectar les incidències a les quals es refereix el fet provat 1r d'aquesta proposta.

Doncs bé, el fet que en les auditories sobre protecció de dades que va dur a terme la CSPT no es detectessin els fets objecte d'imputació, no permeten eximir de responsabilitat a la CSPT.

2.2. Sobre les mesures correctores.

Seguidament, l'entitat imputada adduïa en el seu escrit d'al·legacions davant l'acord d'iniciació que s'havia previst la supressió dels usuaris genèrics, però exposava que la complexitat del projecte, el cost i la situació derivada de l'estat d'alarma, l'havien demorat. No obstant això, la CSPT assenyalava que havia reprès el projecte, el qual s'havia redefinit per fases.

Mentre no s'executa el dit projecte, i per garantir que no es puguin emmagatzemar dades sense necessitat d'autenticar-se, la CSPT manifestava que s'havia ampliat l'espai dedicat als fitxers dels usuaris, el qual sempre requeria l'autenticació mitjançant contrasenya personal.

Així mateix, la CSPT indicava que a través de la intranet s'havia comunicat a tots els empleats que no es podien desar fitxers que continguessin dades personals en el disc dur de l'ordinador, ja que no garantia la seguretat de les dades; que no es podia desar informació amb dades personals fora de les bases de dades corporatives (i que en cas de ser imprescindible, que s'utilitzessin les carpetes de la xarxa); així com que s'havia ampliat l'espai d'emmagatzematge que disposaven els usuaris. Amb contingut similar, la CSPT va enviar un missatge a tots els empleats mitjançant una finestra emergent i va configurar un altre missatge que es mostrava en el moment de posada en funcionament de l'equip informàtic.

D'altra banda, la CSPT també enumerava un seguit de mesures que, al seu criteri, evidenciaven la seva responsabilitat proactiva (l'adhesió a un determinat codi tipus, la realització d'auditories biennals, l'accés per part dels empleats a la guia per a la cura de la confidencialitat, la difusió de novetats sobre protecció de dades a través la intranet, la realització d'auditories mensuals de registre d'accessos, la realització d'activitats formatives sobre protecció de dades, el nomenament d'un delegat de protecció de dades o la realització de diferents procediments interns).

Al respecte, val a dir que les circumstàncies invocades per la CSPT per acreditar la seva responsabilitat proactiva, es podrien tenir en compte per tal de graduar la quantia econòmica de la sanció en cas que aquesta consistís en la imposició d'una multa administrativa, de conformitat amb allò establert a l'article 83.4 de l'RGPD.

Ara bé, en el present cas el règim sancionador aplicable a la CSPT no preveu la imposició d'una sanció econòmica, sinó l'amonestació d'acord amb el previst a l'article 77 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), que per la seva pròpia naturalesa no és susceptible de graduació.

Nogensmenys, tal com assenyalava la persona instructora, correspon destacar i valorar les mesures de responsabilitat proactiva adoptades per l'entitat imputada i les que tenia previst implementar arran els fets objecte del present procediment sancionador, les quals han de permetre (quan estiguin plenament implementades) corregir els efectes de la infracció vinculada al fet provat 1r (l'ús de codis d'usuari i contrasenyes genèrics per iniciar la sessió informàtica a través dels ordinadors de sobretaula, la qual cosa permetia accedir a la unitat local de l'equip en la qual s'emmagatzemaven documents amb dades personals; així com la possibilitat d'accedir remotament al disc dur d'un altre ordinador de la xarxa de la CSPT –la qual cosa s'esmenà durant el mes de març de 2019, aproximadament-).

A l'últim, la CSPT també detallava de forma extensa un seguit d'accions que es van realitzar per incrementar la seguretat de les dades, fruït de l'informe d'anàlisi de riscos.

Doncs bé, en la proposta de resolució es valorava positivament la realització del dit anàlisi de riscos per part de la CSPT (si bé aquest no s'havia aportat).

Dit això, tal com exposava la persona instructora, també és necessari puntualitzar que l'adopció de mesures per corregir els efectes de la infracció no desvirtuen els fets imputats, ni tampoc modifiquen la seva qualificació jurídica.

3. En relació amb les dues conductes descrites a l'apartat de fets provats, cal acudir a l'article 5.1.f) de l'RGPD, que regula el principi d'integritat i confidencialitat determinat que les dades personals seran *"tratados de tal manera que se garantice una seguridad adecuada de los 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".*

Per la seva banda, l'article 32.1 de l'RGPD preveu que *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los 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 (...)."*

Al seu torn, l'article 32.2 de l'RGPD disposa 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 dichos datos."*

Això implica haver de fer una avaluació dels riscos que comporta cada tractament, per determinar les mesures de seguretat que cal implementar.

Sens perjudici de la dita avaluació, l'apartat 2n de la disposició addicional 1a de l'LOPDGDD estableix que *"Els responsables que enumera l'article 77.1 d'aquesta Llei orgànica han d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguin de les que preveu l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents en les empreses o fundacions subjectes al dret privat vinculades a aquells."*

En aquest sentit, l'article 16 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'Administració Electrònica, preveu com un dels requisits mínims de seguretat en allò referent a l'autorització i control dels accessos, que *"El acceso al sistema de información deberá ser controlado y limitado a los*

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

En el present cas, però, l'ús d'un sistema d'identificació i autenticació genèric per iniciar la sessió en els equips informàtics, no garantia el control dels accessos.

Tal com indicava la persona instructora, durant la tramitació d'aquest procediment s'han acreditat degudament les dues conductes descrites a l'apartat de fets provats, que són constitutives de dues infraccions, ambdues previstes a l'article 83.4.a) l'RGPD, que tipifica la vulneració de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43"*, entre les quals hi ha la prevista a l'article 32 RGPD.

Les conductes que aquí s'aborden s'han recollit com a infracció greu a l'article 73.f) de l'LOPDGDD, en la forma següent:

> *"f) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir un nivell de seguretat adequat al risc del tractament, en els termes que exigeix l'article 32.1 del Reglament (UE) 2016/679."*

4. L'article 77.2 LOPDGDD disposa que, en el cas d'infraccions comeses pels responsables o encarregats enumerats a l'art. 77.1 LOPDGDD, l'autoritat de protecció de dades competent:

> *"(...) ha de dictar una resolució que les sancioni amb una amonestació. La resolució ha d'establir així mateix les mesures que escaigui adoptar perquè cessi la conducta o es corregeixin els efectes de la infracció que s'hagi comès.*
> *La resolució s'ha de notificar al responsable o encarregat del tractament, a l'òrgan del qual depengui jeràrquicament, si s'escau, i als afectats que tinguin la condició d'interessat, si s'escau."*

En termes similars a l'LOPDGDD, l'article 21.2 de la Llei 32/2010, determina el següent:

> *"2. En el cas d'infraccions comeses amb relació a fitxers de titularitat pública, el director o directora de l'Autoritat Catalana de Protecció de Dades ha de dictar una resolució que declari la infracció i estableixi les mesures a adoptar per a corregir-ne els efectes. A més, pot proposar, si escau, la iniciació d'actuacions disciplinàries d'acord amb el que estableix la legislació vigent sobre el règim disciplinari del personal al servei de les administracions públiques. Aquesta resolució s'ha de notificar a la persona responsable del fitxer o del tractament, a l'encarregada del tractament, si escau, a l'òrgan del qual depenguin i a les persones afectades, si n'hi ha".*

Tal com s'ha avançat en els antecedents, per mitjà d'escrit de 08/10/2020 la CSPT ha aportat còpia de l'anàlisi de riscos sobre la seguretat de les estacions de treball, motiu pel qual no correspon requerir cap mesura correctora en relació al fet provat 2n.

D'altra banda, en relació a la mesura correctora que proposava la persona instructora en la proposta de resolució pel que fa al fet provat 1r, la CSPT informa en el seu escrit de 08/10/2020 que s'han iniciat les accions correctores oportunes per donar-hi resposta en el termini assenyalat en la proposta de resolució, la qual cosa cal valorar positivament.

Atès l'anterior, escau requerir la CSPT perquè al més aviat possible, i en tot cas en el termini màxim de 3 mesos a comptar des de l'endemà de la notificació d'aquesta resolució, dugui a terme les actuacions necessàries per garantir la identificació i autenticació personalitzada dels usuari autoritzats per accedir als equips informàtics; suprimint els usuaris genèrics ara existents.

Un cop s'hagi adoptat la mesura correctora descrita, en el termini assenyalat, cal que en els 10 dies següents la CSPT n'informi l'Autoritat, sense perjudici de la facultat d'inspecció d'aquesta Autoritat per fer les verificacions corresponents.

## Resolució

Per tot això, resolc:

1. Amonestar la Corporació Sanitària Parc Taulí com a responsable de dues infraccions previstes a l'article 83.4.a) en relació amb l'article 32, ambdós de l'RGPD.

2. Requerir la CSPT perquè adopti la mesura correctora assenyalada al fonament de dret 4t i acrediti davant d'aquesta Autoritat les actuacions dutes a terme per complir-la.

3. Notificar aquesta resolució a la CSPT.

4. Comunicar la resolució que es dicti al Síndic de Greuges, de conformitat amb el que preveu l'article 77.5 de l'LOPDGDD.

5. Ordenar que es publiqui aquesta resolució al web de l'Autoritat (apdcat.gencat.cat), de conformitat amb l'article 17 de la Llei 32/2010, de l'1 d'octubre.

Contra aquesta resolució, que posa fi a la via administrativa d'acord amb els articles 26.2 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, i 14.3 del Decret 48/2003, de 20 de febrer, pel qual s'aprova l'Estatut de l'Agència Catalana de Protecció de Dades, l'entitat imputada pot interposar, amb caràcter potestatiu, un recurs de reposició davant la directora de l'Autoritat Catalana de Protecció de Dades, en el termini d'un mes a comptar des de l'endemà de la seva notificació, d'acord amb el que preveuen l'article 123 i següents de l'LPAC. També pot interposar directament un recurs contenciós

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

administratiu davant els jutjats contenciosos administratius, en el termini de dos mesos a comptar des de l'endemà de la seva notificació, d'acord amb els articles 8, 14 i 46 de la Llei 29/1998, de 13 de juliol, reguladora de la jurisdicció contenciosa administrativa.

Si l'entitat imputada manifesta a l'Autoritat la seva intenció d'interposar un recurs contenciós administratiu contra la resolució ferma en via administrativa, la resolució se suspendrà cautelarment en els termes previstos a l'article 90.3 de l'LPAC.

Igualment, l'entitat imputada pot interposar qualsevol altre recurs que consideri convenient per defensar els seus interessos.

La directora,