Identificación del expediente

Resolución de procedimiento sancionador núm. PS 38/2022, referente al Centro de Telecomunicaciones y Tecnologías de la Información

Antecedentes

1. E n fecha 25/11/2020, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra el Institut Obert de Catalunya (en adelante, el IOC), que es l instituto de enseñanza a distancia del Departamento de Educación, con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales .

En concreto, la persona denunciante, exponía que en fecha 24/11/2020, cuando realizaba el trámite de preinscripción telemática en el IOC, refrescó la página web y "aparecieron los datos personales *de otra persona que no conozco: su nombre y apellidos, su teléfono, su dirección, su fecha de nacimiento, su DNI y su e-mail* ". La persona denunciante aportó documentación sobre los hechos denunciados, en concreto, una imagen de la pantalla del ordenador en el momento en que le apareció la información relativa a "Datos del alumno" *correspondiente* a una tercera persona.

2. La Autoridad abrió una fase de información previa (núm. IP 361/2020), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles motivar la incoación de un procedimiento sancionador.

3. En esta fase de información, en fecha 18/12/2020 se requirió a la entidad denunciada para que informara sobre los motivos que el día 24/11/2020, cuando la persona aquí denunciante tramitaba la preinscripción telemática en el IOC, le aparecieran en pantalla los datos personales de otro usuario, y, también, sobre las medidas de seguridad implementadas por la entidad para proteger la confidencialidad de los datos personales de los alumnos que realicen la preinscripción vía telemática, para evitar el acceso de terceros a estos datos personales .

4. En fecha 04/01/2021, el Departamento de Educación respondió a dicho requerimiento a través de escrito en el que exponía, entre otros, lo siguiente:

- Que *"El día 25 de noviembre de 2020, la delegada de protección de datos del Departamento recibe una comunicación de la dirección del IOC donde se le informa que durante la mañana (del mismo día 25 de noviembre) habían tenido constancia de la existencia de dos incidentes relacionados con los datos que trataban de los futuros alumnos en la Secretaría virtual* ."

- Que " *Ante esta posible violación de seguridad y como responsables del tratamiento de los datos afectados, el director del centro había realizado las siguientes actuaciones:*
  a) Indicó a los alumnos que se estaba gestionando la queja **,** *y que se les informaría de la resolución de la incidencia cuando estuviera solucionada.*
  b) Notificó la incidencia y solicitó ***al Gestor de soluciones al Departamento***

de Educación del CTTI que diera instrucciones inmediatas de bloquear el acceso a la Secretaría *en la que se habían detectado las incidencias. Lo notificaron también a la Subdirección general de Administración y Organización de Centros Públicos.*

c) Recogió evidencias e información relativa al alcance de la incidencia (número de alumnos, tipos de datos a los que se había accedido,...).

d) ***Requirió al Gestor de soluciones al Departamento de Educación del CTTI para que se gestionara la resolución de la incidencia*** *lo antes posible y les confirmara, que estaba solucionada y se podía nuevamente reabrir la Secretaría virtual en condiciones seguras. (...).*

- Que la entidad realizó una serie de actuaciones de investigación sobre los hechos denunciados, *"según el Procedimiento propuesto por la AEPD en la Guía para la gestión y notificación de brechas de seguridad",* de cuyo resultado concluyó que no era necesario notificar la violación de seguridad a la autoridad de control.

- Que " *El mismo día 25 de noviembre por la tarde, el CTTI comunicó que ya había encontrado la incidencia dentro de la aplicación, que también se había revisado la base de datos para ver cuántos casos podrían estar afectados y que sólo tenían uno (el de referencia) y ya se había solucionado. Asimismo, se preparó un paquete de despliegue de la aplicación para que quedara corregido el error y no se pudiera producir ninguna vez más con la previsión de que todo estaría subido al día siguiente a primera hora. "*

- Que " *El día 26 de noviembre, la delegada de protección de datos del Departamento recibe del CTTI la explicación técnica detallada del problema que ya había quedado resuelto: el 24/11/2020, el alumno AAA AAA AAA se dio de alta dos veces de la matrícula, una con un DNI X y su nombre y apellidos y otra con un DNI Y y su nombre y apellidos. Dado que el DNI es el identificador único por la creación de ficha, ambos registros se crearon. Ligado a la matrícula, existe el proceso de creación del username (que también debe ser único), y que se hace con la combinación de nombre y apellido. En el primer caso se crea el username correcto, pero en el segundo, como existe, el sistema da un error generando un username vacío (" "). Por otro lado, el estudiante BBB BBB BBB se registra correctamente por la matrícula y consulta el estado de su matrícula. Mientras tanto, realiza otras actividades, por lo que le salta el time out de la página. El problema en este caso es que en vez de echar al estudiante de su sesión, como hacen otras páginas de la Secretaría (como la de itinerarios), la variable de username deja de tener valor, es decir pasa a estar vacío. Al tener ese username vacío, cuando el usuario refresca la página, se genera una incongruencia entre el valor de la variable y el registro vacío insertado en la doble matrícula anterior (de la AAA AAA AAA) y recupera los datos de otra alumno (de forma aleatoria), que ha sido las de la CCC CCC CCC . De ahí que la alumna BBB BBB BBB pudiera ver los datos de la alumna CCC CCC CCC .*"

- Que " *Para resolver la incidencia se realizaron las siguientes acciones :*
  Se eliminó el valor vacío de la base de datos para que no se pudiera reproducir la situación.
  Se modificó el código fuente de la aplicación a fin de que, aparte de controlar que no se generaran usernames con valor nulo, tampoco se pudieran generar con valor ""). Esta

modificación se llevó a cabo durante la misma mañana del día 26 de noviembre, dejando el problema definitivamente resuelto ."

- La entidad cierra las alegaciones con la siguiente conclusión :
  CONCLUSIÓN *:*
  La causa de la violación de seguridad no provino directamente del IOC sino de su proveedor informático: el CTTI, que sufrió un problema técnico que causó el fallo de seguridad.
  La solución también vino del proveedor informático que detectó la causa técnica y puso la solución en un plazo muy breve .
  El IOC se limitó a trasladar de inmediato la incidencia al proveedor informático, el CTTI y al Departamento de Educación, informó a la delegada de protección de datos, además de tomar las medidas de prevención oportunas (bloquear el acceso a la Secretaría virtual) para impedir que se produjeran nuevas mientras se buscaba la solución, y, finalmente, se excusó ante la persona denunciante en nombre propio y del Departamento."

5. En fecha 22/03/2022, a raíz de la respuesta del IOC del Departamento de Educación en la que señalaba al Centro de Telecomunicaciones y Tecnologías de la Información (en adelante CTTI) como posible responsable de los hechos, se consideró necesario requerir información al CTTI, para que informara, entre otros, sobre lo siguiente:

- si la brecha de seguridad sufrida, que habría propiciado que una persona en el momento de la preinscripción telemática en el IOC pudiera, a través de la web, acceder a los datos vinculados a terceros, se habría producido en el marco de un encargo encomendado al CTTI, y en tal caso, aportara la documentación acreditativa de esta circunstancia (contrato de encargado suscrito con el IOC).
- los motivos que explicarían que el día 24/11/2020, cuando la persona aquí denunciante tramitaba la preinscripción telemática en el IOC, le apareciese en pantalla los datos personales de otro usuario.
- sobre las medidas de seguridad implementadas por el CTTI en la aplicación desarrollada para realizar las preinscripciones telemáticas en el IOC, para evitar el acceso de terceros a estos datos personales.

6. En fecha 26/04/2022, dado que se había superado con creces el plazo concedido sin que el CTTI aportara la información requerida, se reitera el requerimiento al CTTI y se concede un nuevo plazo de 5 días para dar respuesta, con la advertencia expresa de que si no se cumple se podría incurrir en una infracción de la normativa sobre protección de datos de carácter personal.

7. En fecha 02/05/2022, el CTTI dio cumplimiento a este requerimiento mediante escrito a través del cual manifestaba, entre otros, lo siguiente:

- Que " *la brecha de seguridad sufrida se habría producido dentro del marco de la prestación de los servicios TIC que el CTTI realiza en la Generalitat de Catalunya y su Sector Público. En concreto, en el marco del encargo que el Departamento de Educación encomienda al CTTI, puesto que el IOC depende de éste, más concretamente, cuelga de la Dirección General de Centros Públicos. Por este motivo le adjuntamos el acuerdo de encargo de tratamiento de datos de carácter personal vigente entre el CTTI y el Departamento de Educación .*"

- Que " *raíz de una amenaza en el control de cierre de sesión del aplicativo , heredada en el código del aplicativo del anterior proveedor de aplicaciones del CTTI debido a la obsolescencia de versiones en el código del aplicación, se detectó una falta de control de la misma en lo que respecta a la ficha de datos personales de los alumnos. Este hecho provocaba que cuando un alumno perdía la sesión, debido a haber transcurrido un tiempo superior a diez minutos, el aplicativo no lo redirigía a la página de sesión caducada en la que debía volver a iniciar sesión, en lugar de ello, el alumno quedaba en la ficha de datos personales y el código del aplicativo cargaba los datos del siguiente alumno del filtro de búsqueda de estos estudios* ."

- Que " *sobre las medidas de seguridad implementadas, se creó una nueva función en el aplicativo que controla el tiempo de sesión de cada alumno que entra en la ficha de datos personales, con un tiempo máximo de 600 segundos (10 minutos), la que en caso de agotar el tiempo indicado, redirige a los alumnos a la página de sesión expirada de la secretaría del IOC."*

- Que " *a raíz de este hecho, se realizó un análisis en todos los estudios que pudieran sufrir esta carencia en el control de sesiones, a fin de aplicar los mismos cambios en las fichas de datos y otras partes del aplicativo donde se tratan datos de carácter personal y sensible. Por último, sólo fue necesario aplicarlo en la ficha de los estudios reportados.*

  Por último, indicar que tanto la Agencia de Ciberseguridad como el CTTI actúan proactivamente mediante un plan de mitigación de riesgos al respecto de la obsolescencia tecnológica."

El CTTI aportó junto con su escrito de respuesta, copia del documento " *Acuerdo de encargo de tratamiento de datos de carácter personal entre la Administración de la Generalidad, mediante el Departamento de Enseñanza y el Centro de Telecomunicaciones y Tecnologías de la Información de la Generalidad de Cataluña"* , formalizado en fecha 30/03/2016.

En dicho Acuerdo, se establecía en la cláusula primera que el objeto del encargo de tratamiento era el siguiente:

" *Mediante este acuerdo de encargo se habilita al CTTI, en calidad de encargado del tratamiento (en adelante, encargado), para tratar, por cuenta del responsable del tratamiento (en adelante, responsable) los datos de carácter persona necesarios para la gestión centralizada, transversal y coordinada de las soluciones TIC de conformidad con el Acuerdo de Gobierno de 18 de octubre de 2011* ".

Asimismo, en la cláusula tercera, relativa a las obligaciones del encargado del tratamiento, se establecía, entre otras obligaciones, lo siguiente:

i) Cumplir con las medidas de seguridad que corresponden al nivel de seguridad que el responsable ha declarado en el anexo I de este encargo, según lo establecido en la LOPD y el RLOPD y, de acuerdo con las siguientes especificaciones:
(...)
i.7) Aparte de estas especificaciones, el encargado debe implantar el conjunto de medidas previstas para el nivel de seguridad alto en el título VIII del Reglamento de la Ley

orgánica de protección de datos de carácter personal, aprobado por el Reia decreto 1720/2007, de 21 de diciembre ."

En el anexo I de este Acuerdo de encargo, donde se relacionan los ficheros y niveles de protección objeto del encargo de tratamiento, se establece un alto nivel de seguridad para los ficheros relativos a los alumnos de los que sea responsable del fichero la Dirección del IOC.

8 . En fecha 07/06/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el Centro de Telecomunicaciones y Tecnologías de la Información por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 32.1.b); 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). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 09/06/2022.

9. En fecha 20/06/2022, el CTTI formuló alegaciones al acuerdo de iniciación , y aportó una copia del documento "Informe incidencia del servicio", de fecha 15/06/2022.

10. En fecha 23/09/2022, 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 al Centro de Telecomunicaciones y Tecnologías de la Información como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1, ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 23/09/2022 y se concedía un plazo de 10 días para formular alegaciones.

11. El plazo se ha superado con creces y no se han presentado alegaciones.

Hechos probados

El Departamento de Educación (responsable del tratamiento), en virtud del Acuerdo de encargo formalizado en fecha 30/03/2016, encargó al CTTI (encargado del tratamiento) tratar por cuenta del responsable del tratamiento, los datos personales necesarios para la gestión centralizada, transversal y coordinada de las soluciones TIC.

En este Acuerdo, el Departamento de Educación establecía que el CTTI debía implementar las medidas de seguridad previstas en el anexo I del acuerdo, por cada uno de los ficheros allí detallados. En el caso de los alumnos del IOC se preveía que el CTTI debía implementar las medidas de seguridad para el nivel alto, de conformidad con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RLOPD y LOPD, respectivamente)

El CTTI no adoptó las medidas de seguridad adecuadas para garantizar a los alumnos del IOC no pudieran acceder a datos personales de otras personas alumnas. En concreto, en fecha 24/11/2020, mientras la persona denunciante realizaba la preinscripción telemática a una formación ofrecida por el IOC, le apareció en pantalla los datos personales relativos a otro alumno.

Fundamentos de derecho

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

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 lo más relevante de la respuesta motivada de la persona instructora a estas alegaciones.

Al respecto, cabe decir que alegaciones que se formularon en el acuerdo de iniciación no son alegaciones en sí mismas tendentes a cuestionar o desvirtuar la realidad de los hechos que motivaron la incoación del procedimiento, ni su calificación jurídica , sino que se centraban, principalmente, en exponer la medida correctora implementada por la entidad para garantizar que hechos como los aquí probados no vuelvan a suceder.

En este sentido, la entidad, por un lado, reconoce de forma literal " *su responsabilidad respecto a los hechos imputados como encargado del tratamiento de los datos de carácter personal del IOC relacionados en el Anexo 1 del Acuerdo de encargo de tratamiento firmado entre el CTTI y el Departamento de Educación en fecha 30 de marzo de 2016",* y por otro, aporta el documento " *Informe incidencia del servicio* ", donde se recoge la cronología de los hechos, las actuaciones llevadas a cabo a cabo y las acciones correctivas y mejoras implementadas para garantizar que el incidente de seguridad no vuelva a repetirse, y que los alumnos del IOC no puedan acceder telemáticamente a datos personales de otros alumnos. También, informa que, a raíz de los hechos denunciados, la entidad realizó un análisis del resto de aplicaciones del sistema susceptibles de poder sufrir el mismo incidente de seguridad, siendo el resultado final que en ninguno de los casos se repetía la vulnerabilidad de seguridad que habría propiciado que sucedieran los hechos aquí probados. Por último, el CTTI informa, que con la Agencia de Ciberseguridad actúan proactivamente mediante un plan de mitigación de riesgos hacia la obsolescencia tecnológica, así como sobre la aprobación durante el primer trimestre de 2021 del " *Primer Programa de Seguridad del Departamento de Educación* ", donde se establece la creación de un comité de seguridad para poder realizar un seguimiento mucho más esmerado de los riesgos existentes en la ciberseguridad .

A este respecto, cabe señalar que esta Autoridad valora positivamente las diferentes medidas implementadas por la entidad, pero cabe señalar que la adopción de estas medidas no desvirtúan la realidad de los hechos imputados ni la corrección de su calificación jurídica.

3. En relación con los hechos descritos en el apartado de hechos probados, *es* preciso acudir al artículo 5.1.f) del RGPD, que regula el principio de integridad y de confidencialidad

determinante que los datos personales serán *tratados de tal modo 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 (integridad y confidencialidad)".*

Por su parte, el artículo 32.1 del RGPD, en lo referente a la seguridad de los datos, dispone que
Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a las datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento " .

En este caso, en el Acuerdo de encargo del tratamiento de fecha 30/03/2016, el responsable del tratamiento establecía que las medidas de seguridad aplicables a los ficheros relativos a los alumnos del IOC debían ser medidas de seguridad de nivel alto de conformidad con el RLOPD.

A este respecto, cabe tener en cuenta que en la fecha de los hechos denunciados, el contenido del Acuerdo de encargo del tratamiento de fecha 30/03/2016 estaba totalmente vigente, dado que según dispone la disposición transitoria quinta de la LOPDGDD, los contratos de encargado del tratamiento suscritos antes del 25/05/2018 al amparo de lo dispuesto en el artículo 12 de la LOPD, mantenían su vigencia hasta la fecha de vencimiento que señalen y en caso de que se haya pactado de forma indefinida, hasta el 25/05/2022.

Así las cosas, y dado que la vigencia del referenciado Acuerdo de encargo está vinculada al todavía vigente Acuerdo de Gobierno de 18/10/2011, y que no consta que ninguna de las dos partes hayan instado la modificación del Acuerdo de encargo para adecuarlo a lo dispuesto en el artículo 28 del RGPD, se considerará que dicho Acuerdo de encargo siguió vigente hasta el día 25/05/2022, sin que le fuera exigible adecuar su contenido en el artículo 28 del RGPD.

No obstante, debe indicarse que, con independencia de la vigencia del referenciado Acuerdo de encargo, a partir de la entrada en vigor del RGPD (25/05/2018), sí que debían ser aplicadas las medidas de seguridad derivadas del RGPD. Es decir, aquellas medidas de seguridad las cuales, a raíz de una valoración previa de riesgos (art. 32 del RGPD), se consideraran apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Por tanto, el CTTI debía implementar, en relación con el tratamiento de los datos personales de los alumnos del IOC, las medidas de seguridad de nivel alto que comportaba su tratamiento .

A este respecto, hay que tener en cuenta que la disposición adicional primera de la LOPDDDD establece lo siguiente: " *El Esquema Nacional de Seguridad debe incluir las medidas que deban implantarse en caso de tratamiento de datos personales para evitar -la pérdida, alteración o acceso no autorizado, con la adaptación de los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679"* .

Pues bien, respecto a la conducta descrita en el apartado de hechos probados, se infiere que la entidad imputada vulneró la medida de seguridad prevista en el artículo 16 del Esquema Nacional de Seguridad vigente en ese momento (RD 3/ 2010, de 8 de enero), precepto que regula la autorización y el control de los accesos en los siguientes términos: " *El acceso al sistema de información debe ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas* ."

En este sentido, cabe indicar que cuando se formalizó el Acuerdo de encargo entre el Departamento de EDU y el CTTI (2016), el cumplimiento de las medidas de seguridad relativas a la autorización y al control de accesos recogía en el Anexo I de dicho Acuerdo de encargo. Esto es así porque en el Anexo I, ya se establecía que, en relación con el tratamiento de los datos personales de los alumnos del IOC , debían implementarse las medidas de seguridad de nivel alto. Al respecto, debe indicarse que, en ese momento, el cumplimiento de las medidas de seguridad de nivel alto comportaba de forma acumulativa el cumplimiento de las medidas de seguridad de nivel básico y medio. Por tanto, se consideraba incluido el cumplimiento de las medidas de seguridad relativas al control de accesos y la identificación y autenticación, previstas como medidas de seguridad de nivel básico en los artículos 91 y 93 del RLOPD, respectivamente.

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, que es constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de *las obligaciones del responsable y del encargado* , entre las que se encuentra la recogida en el artículo 32 .1.b del RGPD arriba transcrito, referente a la seguridad del tratamiento que garantice la confidencialidad, integridad, disponibilidad *y* resiliencia permanentes de los sistemas y servicios del tratamiento.

La conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"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 del Reglamento (UE) 2016/679"

4. Al tratarse el CTTI de una entidad de derecho público adscrita a la Secretaría de Políticas Digitales del Departamento de Territorio, le resulta de aplicación el régimen previsto en el artículo 77 LOPDGDD para determinadas categorías de responsables o encargados del tratamiento, entre ellos, las entidades de derecho público vinculadas o dependientes de las administraciones públicas.

En este sentido, 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".*

En el presente caso, resulta innecesario requerir medidas correctoras de los efectos de la infracción dado que las medidas adoptadas por el CTTI se consideran suficientes y adecuadas para garantizar que en un futuro se repitan hechos similares a los aquí probados.

Por todo esto, resuelvo:

1. Amonestar en el Centro de Telecomunicaciones y Tecnologías de la Información como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1, ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 4º.

2. Notificar esta resolución en el Centro de Telecomunicaciones y Tecnologías de la Información.

3. Comunicar la resolución al Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD.

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

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

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

La directora,