- **Expediente N.º: EXP202201172**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 24 de enero de 2022, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por SERVICIO DE SALUD CASTILLA LA MANCHA TALAVERA con NIF Q4500146H (en adelante, SESCAM Talavera), recibido en fecha 23 de diciembre de 2021, en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

En la citada fecha, 23 de diciembre de 2021, tiene entrada la notificación de la primera de las brechas de seguridad (en adelante Brecha 1) por parte del SESCAM Talavera. El incidente de seguridad está relacionado con un acceso ilegítimo a la historia clínica de un paciente por parte de una profesional trabajadora del SESCAM Talavera sin tener vinculación asistencial alguna con el mismo. El incidente es detectado a raíz de la reclamación/queja presentada por el paciente afectado en el Hospital de Talavera de La Reina. En ella denuncia que, tras estar ingresado en ese hospital durante varios días de septiembre de 2021, su exmujer, Auxiliar de Enfermería del mismo, había accedido a su historia clínica y a sus datos de salud de forma indebida y que había difundido esta información a terceras personas incluso antes de que el propio médico le diera el diagnóstico.

Indican que la fecha de detección de la brecha es el 17 de diciembre de 2021 (estimada), que los hechos comenzaron a tener lugar el 9 de septiembre de 2021 y que la queja del paciente afectado fue presentada el 8 de octubre de 2021. SESCAM Talavera remite escrito al Juzgado Guardia de Instrucción de Talavera denunciando los accesos indebidos. En fecha 23 de diciembre de 2021 se comunica e informa sobre la brecha a la persona afectada.

Con fecha 28 de diciembre se recibe en el registro electrónico de esta Agencia ampliación sobre la Brecha 1, en concreto se aporta, por parte del director Gerente de la Gerencia de Atención Integrada de Talavera de la Reina, la siguiente documentación:

- Formulario interno del SESCAM Talavera para la notificación de brecha de seguridad.
- La queja del propio paciente afectado con entrada en registro del 8 de octubre de 2021.

- Informe del Servicio de Informática del SESCAM Talavera con el listado de los accesos a la historia clínica del afectado por parte de la profesional Auxiliar de Enfermería, de 3 de diciembre de 2021.

- Escrito de denuncia penal dirigido por parte del SESCAM Talavera al juzgado de guardia de instrucción de Talavera, firmado el 20 de diciembre de 2021

- Remisión de escritos internos a la Delegación Provincial de Sanidad (con una propuesta de instrucción sancionadora) y a la Gerencia de Inspección (para posibles investigaciones pertinentes), de fechas 29 y 25 de noviembre de 2021 respectivamente.

SEGUNDO: Con fecha 29 de diciembre de 2021 se recibe por el mismo responsable una segunda notificación de brecha de seguridad (en adelante Brecha 2) en el registro de esta Agencia. Se informa en la misma del acceso indebido a historias clínicas de pacientes por parte de un médico del SESCAM Talavera en situación de suspensión firme de funciones por sanción disciplinaria. Se detecta a raíz de una notificación por parte de otro profesional médico del mismo consultorio local donde tuvieron lugar los hechos. Se trata del acceso a datos de salud de unos 60 afectados (aproximadamente). La fecha de detección es el 27 de diciembre de 2021 (fecha exacta) y la fecha en la que tuvo comienzo el incidente es el 11 de octubre de 2021. No se comunica a los afectados porque, según consideran, no existe un riesgo alto para los derechos y libertades de los afectados al ser todos ellos pacientes del propio profesional médico.

TERCERO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

Teniendo en cuenta la documentación proporcionada en las notificaciones de las brechas, con fecha 21 de febrero de 2022 se efectúa requerimiento de información para que se aclaren algunos aspectos de ambas brechas, recibiéndose contestación por parte de SESCAM Talavera en fecha 14 de marzo de 2022. De dicha contestación se obtiene la siguiente información:

En relación con la Brecha 1:

- Con fecha 19 de octubre de 2021 tiene entrada en el Comité de Gestión de la Seguridad de la Información del SESCAM Talavera (en adelante COMITÉ), encargado de gestionar las brechas de seguridad, la queja formulada por el afectado el 8 de

octubre de 2021 y se procede a solicitar al servicio de informática y documentación clínica el listado de accesos a historias clínicas

- Con fecha 24 de noviembre de 2021 se recibe del servicio de informática informe de 38 páginas en formato electrónico, pero este informe no estaba depurado y se vuelve a solicitar subsanación al citado servicio.

- Con fecha 25 de noviembre de 2021 el COMITÉ da traslado de las sospechas de acceso indebido a la Gerencia de Coordinación e Inspección Médica del SESCAM Talavera para que actúen en consecuencia.

- Con fecha 29 de noviembre de 2021 el COMITÉ da traslado a las autoridades competentes para imponer sanciones disciplinarias de la Consejería de Sanidad de la JJ.CC – Castilla La Mancha para que actúen en consecuencia, remitiéndose el listado de accesos no depurado.

- Con fecha 3 de diciembre de 2021 el COMITÉ recibe contestación de la Gerencia de Coordinación e Inspección Médica indicando la falta de competencias para actuar en este asunto, ya que la profesional denunciada ya no tiene contrato vigente en esta fecha, pues su contrato finalizó el 30 de septiembre de 2021.

- Con fecha 17 de diciembre de 2021 el COMITÉ recibe informe de la Dirección de Enfermería sobre los puestos de trabajo que había desempeñado la profesional denunciada en los días 9, 10 y 13 de octubre de 2021. El objeto de este informe es conocer si los accesos a la historia clínica tenían relación con una posible asistencia médica que la profesional estuviera prestando y por tanto no debía considerarse acceso indebido al historial clínico. En el mismo se confirma que los accesos de los días 9 y 10 de octubre de 2022 no tienen ninguna posible vinculación asistencial, sin embargo, el día 13 de octubre la profesional había estado trabajando en la misma planta donde estaba ingresado el paciente, aunque no se confirma que existiera vinculación asistencial al no poderse demostrar que era un paciente asignado a la misma.

- Con fecha 20 de diciembre de 2021 se recibe en COMITÉ el informe depurado en formato electrónico del servicio de informática, resultando accesos bajo sospecha en 2021 y descartándose los de 2020. La información que contiene es la misma que el informe no depurado a excepción de que está filtrada para mostrar los accesos a la historia clínica del paciente afectado por parte de la profesional Auxiliar de Enfermería. La fecha de emisión que tiene grabada el informe es del 03 de diciembre de 2021.

- Con fecha 23 de diciembre de 2021 se presenta escrito de denuncia penal en juzgado de instrucción de Talavera. También en esta misma fecha se hace la correspondiente notificación de la brecha ante esta Agencia.

En relación con la Brecha 2:

- Con fecha 22 de noviembre de 2021 tiene entrada en el COMITÉ la comunicación por parte de un profesional médico del SESCAM Talavera informando sobre un presunto acceso indebido a historias clínicas por parte de otro profesional médico estando éste suspendido en funciones por un periodo de tres meses (desde el 11 de octubre de 2021 al 11 de enero de 2021). El COMITÉ se comunica con el denunciante para aclarar sobre el retraso en la comunicación, ya que los hechos suceden el 11 de octubre de 2021 y se comunica el 22 de noviembre de 2021.

- Con fecha 22 de noviembre de 2021 el COMITÉ solicita al servicio de informática el listado de accesos a los sistemas por parte de este profesional denunciado.

- Con fecha 25 de noviembre de 2021 se remite la información a la Gerencia de Inspección Médica del SESCAM Talavera, como órgano competente a efectos de sanciones disciplinarias.

- Con fecha de 28 de diciembre de 2021 se recibe por parte del servicio de informática el informe de accesos solicitado.

- Con fecha 29 de diciembre de 2021, tras conocer el informe de informática, se declara la brecha de seguridad y se notifica ante esta Agencia.

Preguntado por la dilación en el tiempo en relación con la notificación a la Agencia de la Brecha 1, contestan que finalmente la fecha de detección no es el 17 de diciembre 2021 como indicaron en formulario de notificación, sino el 20 de diciembre de 2021, momento en que se recibe el listado filtrado por parte del servicio de informática.

Preguntado por la falta de comunicación con los afectados en Brecha 2, contestan que no es necesaria tal comunicación puesto que todos son pacientes del propio profesional médico suspendido en funciones.

Preguntado por el análisis de riesgos, aportan documento del último análisis realizado, con fecha de 30 de diciembre de 2015, indicando que se realizó de manera conjunta para dar cumplimiento tanto al Esquema Nacional de Seguridad como al RGPD.

Preguntado por las medidas preventivas y correctivas establecidas, contestan que las medidas implantadas son las detalladas en la auditoría llevada a cabo en 2018 y cuyo informe aportan a esta investigación. Indican que esta auditoría se enmarca en lo previsto en el Esquema Nacional de Seguridad y se realiza entre los meses octubre y diciembre de 2018. Del informe de esta auditoría se desprende que el resultado fue "Favorable con No Conformidades" y la recomendación para llevar a cabo una serie de acciones correctivas. ***(…)***

Existe una política de seguridad y protección de datos con fecha de publicación de noviembre de 2019 donde se establece una estructura organizativa formada por:

- El Responsable de Seguridad.
- El Comité Técnico de Seguridad de la Información (actúa de DPD).
- El Equipo de Seguridad.
- Comité de Gestión de la Seguridad de la Información (existente en el ámbito de cada Gerencia del SESCAM Talavera, entre sus funciones destaca el registro de las incidencias de seguridad y el control periódico de la revisión del control de accesos a los sistemas de información)

Preguntado por el motivo por el cual las medidas establecidas no evitaron el incidente, contestan:

- Para la Brecha 1 indican que no es posible restringir el acceso a la historia de los pacientes de manera tan exhaustiva, como por ejemplo a nivel de planta, y que por ello y como contramedida, la trazabilidad y control del acceso de los profesionales es exhaustiva.

- Para la Brecha 2 indican que el incidente se produce porque la gerencia no gestionó correctamente la baja del profesional suspendido en funciones.

Preguntado por los perfiles existentes para acceder al sistema, contestan que los roles de acceso están vinculados con la categoría profesional de la persona. La categoría

profesional Auxiliar de Enfermería podía tener acceso completo de consulta a cualquier historia clínica. Los usuarios se autentican en el sistema con un usuario registrado en el directorio LDAP corporativo y es en este directorio donde se almacena la categoría profesional del mismo y consecuentemente los roles de acceso y visibilidad del aplicativo. Con respecto a la gestión de las bajas de usuarios, indican que es realizada de forma manual por la gerencia a través de la aplicación GesUser.

Preguntado por la Evaluación de Impacto, responden que no existe puesto que los sistemas de consultas de historias clínicas datan de 2005 y 2008 y que, por lo tanto, eran anteriores a la actual normativa de protección de datos.

- En relación con la NOTIFICACIÓN DE LA BRECHA cabe destacar:

  - Con respecto a la Brecha 1, hay evidencias suficientes para determinar que con fecha 17 de diciembre de 2021 el responsable de tratamiento tenía constancia de que el incidente de seguridad (notificada el 23 de diciembre de 2021) había afectado a datos personales, ya que fue en esta fecha cuando se recibió el informe por parte de la Dirección de Enfermería afirmando que los accesos a la historia clínica de los días 9 y 10 de octubre no tenían vinculación asistencial entre el paciente y la profesional. Cabe resaltar también que esta fecha de detección pudo haber sido bastante anterior -y por consiguiente no se hubiera dilatado tanto en el tiempo desde que se recibe la queja del paciente hasta que se detecta-, si hubiesen existido medidas organizativas ágiles y eficientes para la comunicación y flujos de información entre el propio Comité de Gestión de Seguridad de la Gerencia y el Servicio de Informática o la Dirección de Enfermería, canalizándose la información solicitada/recibida entre ellos de una forma rápida.

  - Con respecto a la Brecha 2, la notificación de esta ante esta Agencia se llevó a cabo sin dilación indebida.

- En relación con la COMUNICACIÓN CON LOS AFECTADOS cabe destacar:

  - Con respecto a la Brecha 1, la comunicación con el único afectado fue correcta en tiempo y forma, sin dilación indebida y ajustándose a lo establecido.

  - Con respecto a la NO comunicación de los afectados en la brecha 2, no existe probabilidad de que dicha violación entrañe alto riesgo para los derechos

y libertades de los afectados al tratarse todos ellos de pacientes del propio profesional sancionado y, por tanto, esta información ya era conocida por este de forma autorizada.

- En relación con las MEDIDAS TÉCNICAS Y ORGANIZATIVAS para garantizar un nivel de seguridad adecuado al riesgo:

La normativa actual de protección de datos se fundamenta en un modelo basado en la responsabilidad proactiva por parte de los responsables de tratamiento, los cuales deben incorporar medidas técnicas y organizativas que aseguren la protección de los datos personales objeto de tratamiento, no solo teniéndose esto en cuenta desde el diseño y por defecto para la puesta en funcionamiento de nuevos sistemas de información que sirvan de base en el tratamiento, sino también para cualquier sistema implantado previamente a la actual normativa y a través de los correspondientes análisis de adecuación de los mismos. Para el caso de organismos públicos, estas medidas serán las incluidas en el Esquema Nacional de Seguridad, y deben ser justificadas en proporción con los riesgos analizados, análisis obligatorio y que puede realizarse de manera conjunta con el establecido por el RGPD. Teniéndose todo ello en cuenta se concluye:

- No existe Análisis de Riesgos para dar cumplimiento a la actual normativa de protección de datos.

- Como consecuencia de lo anterior, muchas de las medidas técnicas y organizativas implantadas son inexactas o insuficientes, especialmente:

  - ***(…)***

Con respecto a lo anterior, se puede tener en cuenta el trabajo del antiguo Grupo de Trabajo 29 WP 131, “Sobre el Tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)”, trabajo que, aunque es anterior a la vigente normativa de protección de datos, hace un buen análisis sobre las garantías generales relativas al acceso a los historiales médicos por parte de los profesionales. En el punto 3 del mismo (“Reflexión sobre un marco jurídico adecuado para los sistemas de historias clínicas”) se indica:

“*Los datos contenidos en los sistemas de Historiales Médicos Electrónicos (HME) son historiales médicos confidenciales. Por tanto, el principio esencial*

relativo al acceso a un HME debe ser que, aparte del propio paciente, sólo podrán tener acceso al mismo aquellos profesionales de la salud/personal autorizado de instituciones sanitarias que participen en ese momento en el tratamiento del paciente. Debe existir una relación de tratamiento médico real y actual entre el paciente y el profesional de la salud que desee acceder a su HME. Parece también necesario regular qué categorías de profesionales sanitarios/instituciones y a qué nivel pueden acceder a datos de los HME (¿médicos generalistas, médicos de hospital, farmacéuticos, enfermeras, quiroprácticos? ¿psicólogos? ¿terapeutas familiares? etc.). La protección de los datos podría asimismo verse reforzada mediante unos derechos de acceso modulares, esto es, creando en un sistema de HME categorías de datos médicos de forma que el acceso esté limitado a categorías específicas de profesionales o instituciones sanitarias."

Con respecto a esto, cabe añadir también lo indicado en el informe emitido por el gabinete jurídico de esta Agencia (Informe 656/2008) ante una consulta planteada sobre el acceso a las historias clínicas de un hospital por determinados profesionales cuya categoría profesional no estaba relacionada con la asistencia médica del afectado. Este informe concluye reflexionando sobre lo especificado en el trabajo WP131:

"En consecuencia, como regla general, el acceso a la historia clínica en el ámbito de un determinado centro sanitario quedará limitado a:

- *El propio personal sanitario que preste asistencia al paciente, a fin de garantizar su adecuado diagnóstico y tratamiento.*
- *El personal de administración y gestión, exclusivamente en lo que resulte necesario para el ejercicio de sus propias funciones.*
- *Fuera de estos casos, será preciso, como regla general, el consentimiento del paciente."*

Añadir también a esta investigación que, según lo dispuesto en la Ley 44/2003, de 21 de noviembre, sobre ordenación de las profesiones sanitarias, la categoría profesional "Auxiliar de Enfermería" pertenece a "profesionales del área sanitaria de formación profesional". Por el contrario, la categoría "Enfermería" pertenece a "profesiones sanitarias reguladas". Este último tipo ostentaría el derecho de acceso a la historia clínica del paciente siempre que se cumplan los requisitos de que el acceso se realice para garantizar una asistencia adecuada al paciente y que los datos de la historia constituyan un instrumento fundamental para su adecuada asistencia.

Por lo tanto, y concluyendo la investigación, a la hora de establecer medidas para restringir el acceso a las historias clínicas de pacientes en función del perfil profesional del usuario, habría que tener en cuenta la

diferenciación entre las distintas categorías profesionales, así como también la vinculación asistencial que estos tengan con el paciente. No parece razonable que una profesional con perfil “Auxiliar de Enfermería” pueda tener acceso al historial médico completo de un determinado paciente con el que no tiene vinculación asistencial. No obstante, si no se utilizan medidas técnicas restrictivas para impedir este acceso, sería imprescindible activar contramedidas de trazabilidad más rígidas y eficaces que las actualmente existentes, minimizando los efectos de la consulta indebida y mitigando el riesgo al reducir el impacto de la brecha.

- Las medidas existentes para bloquear las sesiones abiertas inactivas de los usuarios profesionales que se ausentan no parecen ser suficientes. En la Brecha 2, el profesional (en suspensión de funciones) se personificó en el despacho que previamente había abandonado otro profesional médico dejando este su sesión abierta. Por otro lado, el informe de auditoría de 2018 hace referencia a la inexistencia de medidas para bloquear sesiones abiertas inactivas y propone como medida correctiva aplicar un factor de tiempo de 5 minutos para que se cierren las sesiones que no muestren señales de actividad.

- Por la información aportada, hay evidencias para concluir que las medidas organizativas establecidas para gestionar las brechas de seguridad son insuficientes, sobre todo en los procedimientos establecidos para solicitar y recibir información entre departamentos o unidades distintas. Como ejemplo, cabe mencionar la recepción por parte del Comité de Gestión de la Seguridad del listado de accesos realizados por un determinado profesional a los sistemas de historias clínicas de un paciente concreto, tardándose casi un mes en recibir dicho listado por parte del servicio de informática, además este informe recibido contenía defectos y no se ajustaba a lo solicitado, por lo que las vías y canales establecidos para solicitar y recibir información no son los adecuados para una eficiente gestión de los incidentes.

- En relación con la EVALUACIÓN DE IMPACTO de los tratamientos de datos personales afectado por la brecha:

No existe evaluación de impacto para los tratamientos de datos. Justifican esta inexistencia en que se trata de sistemas de información implantados con anterioridad a la actual normativa de protección de datos (años 2005 y 2008). El informe de la Agencia de Protección de Datos “El impacto del Reglamento General de Protección de Datos sobre la actividad de las administraciones públicas” menciona la necesidad de valorar si los tratamientos que se realizan requieren una evaluación de impacto sobre la protección de datos personales al suponer un alto riesgo para los derechos y libertades de los interesados, así

como disponer una metodología para llevarlo a cabo. Por otro lado, el informe de auditoría de 2018 aportado menciona como una de las medidas correctivas la necesidad de realizar una evaluación del cumplimiento de estos sistemas a la actual normativa, evaluación que debe concluir con un plan de adecuación.

Esta evaluación de impacto es necesaria puesto que existe alto riesgo para los derechos y libertades para las personas físicas. La LOPDGDD incluye en el apartado segundo del artículo 28 una serie de supuestos que podrían entrañar un riesgo elevado, entre los que se especifican algunos que podrían ser predicables del tratamiento de datos de salud a propósito de la historia clínica, como señala en su letra a) con respecto a la perdida de confidencialidad de datos sujetos al secreto profesional, o incluso en la letra c) del mismo artículo, en lo referente al tratamiento no incidental de datos especialmente protegidos por el artículo 9 del RGPD, entre los que se encuentran los datos de salud.

- Conclusiones:

  - Hay evidencias para afirmar que a fecha 17 de diciembre de 2021 el responsable tenía constancia de que los accesos de la profesional a la historia clínica del paciente no tenían vinculación asistencial y por lo tanto se trataba de un acceso ilegítimo. Existiendo por tanto retraso en la notificación de la brecha.

  - No existe análisis de riesgos para adaptar los tratamientos de datos personales a la actual normativa.

  - La trazabilidad y supervisión de los accesos realizados en el sistema para consultar las historias clínicas es insuficiente.

  - Los procesos de gestión de bajas de usuarios no están documentados, debiéndose implantar procedimientos formales.

  - Las medidas organizativas para gestionar las posibles brechas de seguridad por accesos indebidos son ineficientes, sobre todo en lo relativo a los canales de comunicación establecidos entre el servicio de informática y el Comité responsable de gestionar la brecha.

- No existe evaluación de impacto para los tratamientos de datos.

TERCERO: Con fecha 12 de septiembre de 2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a SESCAM Talavera, por las presunta infracciones de los artículos 5.1.f), tipificada en el artículo 83.5 del RGPD; artículo 32, artículo 33 y artículo 35 del RGPD, tipificadas en el artículo 83.4 del RGPD.

El acuerdo de inicio fue notificado electrónicamente a la SESCAM Talavera. Así lo exige el artículo 14.2 de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) conforme al cual "*En todo caso estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos: a) Las personas jurídicas".*

Obra en el expediente Certificado emitido por el Servicio de Notificaciones Electrónicas y de Dirección Electrónica Habilitada de la FNMT-RCM, que deja constancia del envío del acuerdo de inicio, notificación de la AEPD dirigida a SESCAM Talavera, a través de ese medio siendo la fecha de puesta a disposición en la sede electrónica del organismo el 13 de septiembre de 2022 y la fecha de rechazo automático el día 24 del mismo mes y año
.
El artículo 43.2. de la LPACAP establece que cuando la notificación por medios electrónicos sea de carácter obligatorio -como acontece en el presente caso- "*se entenderá rechazada cuando hayan transcurrido diez días naturales desde la puesta a disposición de la notificación sin que se acceda a su contenido*." (El subrayado es nuestro)

Añadir que los artículos 41.5 y 41.1, párrafo tercero, de la LPACAP establecen, respectivamente, que:

Cuando el interesado o su representante rechace la notificación de una actuación administrativa, se hará constar en el expediente especificándose las circunstancias del intento de notificación y el medio, dando por efectuado el trámite y siguiéndose el procedimiento. (El subrayado es nuestro)

Con independencia del medio utilizado, las notificaciones serán válidas siempre que permitan tener constancia de su envío o puesta a disposición, de la recepción o acceso por el interesado o su representante, de sus fechas y horas, del contenido íntegro, y de la identidad fidedigna del remitente y del destinatario de la misma. La acreditación de la notificación efectuadas se incorporará al expediente.

CUARTO: El artículo 73.1 de la LPCAP determina que el plazo para formular alegaciones al Acuerdo de Inicio es de diez días computados a partir del siguiente al de la notificación.

El artículo 64.2.f) LPACAP establece que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada". (El subrayado es de la AEPD).

En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a SESCAM Talavera y la sanción que podría imponerse. Por ello, tomando en consideración que SESCAM Talavera no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes

HECHOS PROBADOS

PRIMERO: Respecto de la Brecha 1, se produjeron accesos a la historia clínica de un paciente por parte de una auxiliar de enfermería del hospital en el que se encontraba ingresado, sin que hubiera una justificación asistencial para ello, accediendo, por tanto, a datos de salud de dicho paciente. Así lo corrobora el informe de informática que obra en el expediente en el que se constatan accesos producidos el 1 de abril y los días 9, 10 y 13 de septiembre de 2021, junto con el informe de la Dirección de Enfermería.

En cuanto a la Brecha 2, se produjeron dos accesos por parte de un médico al historial de sus pacientes (unos 60), aprovechando la sesión abierta de otro profesional médico, los cuales ocurrieron los días 11 de octubre y 22 de noviembre de 2021, cuando el mismo se encontraba suspendido en funciones.

Estos accesos ilícitos han afectado a los datos de salud contenidos en las historias clínicas de los afectados.

SEGUNDO: De lo manifestado por SESCAM Talavera y de la documentación que obra en el expediente, respecto de las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de los datos personales, ha quedado acreditado lo siguiente:

- ***(…)***

- En la Brecha 2, el profesional (en suspensión de funciones) se personificó en el despacho que previamente había abandonado otro profesional médico dejando este su sesión abierta y siendo ello aprovechado para acceder al historial médico de sus pacientes. ***(…).***

- En la Brecha 1, desde que se presentó la queja hasta que se determinó que se había producido una violación de la seguridad por accesos indebidos, pasaron más de dos meses. Por tanto, las medidas organizativas para gestionar incidentes de seguridad son insuficientes.

TERCERO: Respecto de la Brecha 1, el SESCAM Talavera ha sufrido una brecha de seguridad de los datos personales, que tuvo lugar el 9/09/2021 y de la que el responsable ya tenía constancia de ella el 17/12/2021 (fecha de recepción del Informe de Enfermería), no habiendo notificado la misma a esta Agencia hasta el 23/12/2021, sin haber acreditado los motivos que justifiquen tal dilación.

CUARTO: SESCAM Talavera, como responsable de tratamiento, trata datos de salud y a gran escala. Sin embargo, en el momento de producirse la brecha, no tiene realizada una Evaluación de Impacto para la Protección de Datos respecto de los tratamientos afectados por la misma.

FUNDAMENTOS DE DERECHO

I
Competencia

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que SESCAM Talavera realiza, entre otros tratamientos, la recogida, registro, organización, conservación, consulta, acceso, utilización y supresión de los siguientes datos personales de personas físicas, tales como: nombre, apellidos, número de identificación, datos de contacto, datos de salud, etc.

SESCAM Talavera realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante brecha de seguridad) como “todas

aquellas violaciones de la seguridad que ocasionen 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."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad al haberse producido accesos indebidos a la historia clínica de pacientes por parte de personal sin existir justificación asistencial de carácter médico para ello en el momento de los accesos.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Artículo 5.1 f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) 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 («integridad y confidencialidad»)."

En el presente caso, consta que los datos de salud de los afectados, obrantes en la base de datos del SESCAM Talavera, fueron indebidamente expuestos a terceros, al producirse un acceso no autorizado o ilícito, vulnerándose con ellos su carácter confidencial.

Así, respecto de la Brecha 1, se produjeron accesos a la historia clínica de un paciente por parte de una auxiliar de enfermería del hospital en el que se encontraba ingresado sin que hubiera una justificación asistencial para ello, accediendo, por tanto, a datos de salud de dicho paciente. Así lo corrobora el informe de informática que obra en el expediente en el que se constatan accesos producidos el 1 de abril y los días 9, 10 y 13 de septiembre de 2021.

En cuanto a la Brecha 2, se produjeron dos accesos por parte de un médico al historial de sus pacientes (unos 60), los cuales ocurrieron los días 11 de octubre y 22 de noviembre de 2021, cuando el mismo se encontraba suspendido en funciones.

En este sentido, no debe olvidarse, tal y como ha quedado expuesto en las actuaciones de investigación indicadas en el Antecedente de Hecho Tercero, que las medidas técnicas y organizativas no eran las apropiadas para garantizar una seguridad adecuada de los datos personales, en especial para la protección contra el tratamiento no autorizado o ilícito, teniendo en cuenta el carácter confidencial de los datos personales, especialmente los datos de salud.

De conformidad con las evidencias de las que se dispone, los hechos conocidos son constitutivos de una infracción, imputable a SESCAM Talavera, por vulneración del artículo 5.1.f) del RGPD.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

V
Sanción por la infracción del artículo 5.1.f) del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"*7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"*1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*

> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 5.1.f) del RGPD, corresponde sancionar con un apercibimiento a SESCAM Talavera.

VI
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. 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, 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 los 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.*

2. 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

El artículo 32 no establece medidas de seguridad estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

En consonancia con estas previsiones, el Considerando 75 del RGPD establece: Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen

aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

Asimismo, el Considerando 83 del RGPD establece: A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad, tanto técnicas como organizativas, son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

En este sentido, procede señalar que la actividad que realiza el SESCAM Talavera conlleva el tratamiento a gran escala de datos relativos a la salud.

Por ello, derivado de la actividad a la que se dedica y de los datos personales que trata, el SESCAM Talavera está obligado realizar un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las

personas, teniendo en cuenta especialmente que su actividad conlleva tratar datos personales relativos a la salud.

En el presente caso, tal y como se ha detectado tras las actuaciones de investigación, el SESCAM Talavera no cuenta con las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, muchas de ellas derivadas de la no existencia de un análisis de riesgos para dar cumplimiento a la actual normativa de protección de datos. A destacar:

- ***(…)***

De conformidad con las evidencias de las que se dispone, los hechos conocidos son constitutivos de una infracción imputable a SESCAM Talavera por vulneración del artículo 32 del RGPD.

VII
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)”*

A este respecto, la LOPDGDD, en su artículo 71 “*Infracciones*” establece que “*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.*

A efectos del plazo de prescripción, el artículo 73 “*Infracciones consideradas graves*” de la LOPDGDD indica:

“En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

VIII
Sanción por la infracción del artículo 32 del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.5 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"*1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados*:

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 32 del RGPD, corresponde sancionar con un apercibimiento al SESCAM Talavera

IX
Artículo 33 del RGPD

El Artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD establece:

"1. *En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación*.

2. *El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.*

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

> *a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
> *b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
> *c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
> *d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, respecto de la Brecha 1, consta que el SESCAM Talavera ha sufrido una brecha de seguridad de los datos personales, que tuvo lugar el 9/09/2021 y

de la que el responsable ya tenía constancia de ella el 17/12/2021, no habiendo informado de ella a esta Agencia hasta el 23/12/2021, sin haber acreditado los motivos que justifiquen tal dilación.

A pesar de que por parte del responsable se afirma que la fecha a tener en cuenta es el 20/12/2021, que es cuando reciben el informe depurado del departamento de informática, es realmente con el Informe de Enfermería, recibido el 17/12/2021, que afirma que los accesos a la historia clínica de los días 9 y 10 de octubre de 2021 no tienen vinculación asistencial entre el paciente y la profesional, cuando el SESCAM Talavera tiene constancia de la existencia de la brecha de seguridad (amen de resaltar, como ya se ha señalado anteriormente, de que esa fecha debería y podría haber sido mucho anterior si hubieran existido medidas organizativas adecuadas para gestionar la brecha de seguridad)

En cuanto a la Brecha 2, la notificación del incidente de seguridad se llevó a cabo de conformidad con el artículo 33 del RGPD.

De conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable al SESCAM Talavera, por vulneración del artículo 33 del RGPD.

X
Tipificación de la infracción del artículo 33 del RGPD

La citada infracción del artículo 33 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 74 "*Infracciones consideradas leves*" de la LOPDGDD indica:

"*Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*
(…)

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

XI
Sanción por la infracción del artículo 33 del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.4 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 33 del RGPD, corresponde sancionar con un apercibimiento a SESCAM Talavera

XII
Artículo 35 del RGPD

El Artículo 35 "*Evaluación de impacto relativa a la protección de datos*" del RGPD establece:

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

> *a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*
> *b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*
> *c) observación sistemática a gran escala de una zona de acceso público.*

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta

de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

> *a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;*
> *b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;*
> *c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y*
> *d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.*

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

Conforme lo dispuesto en el art 35.4 del RGPD, la AEPD ha establecido y publicado una
lista de los tipos de operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos (en adelante EIPD), entre las que se encuentra:

4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD…
6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.
7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 <<*Directrices sobre la evaluación de impacto relativa a la protección de datos y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679*", los complementa y debe entenderse como una lista no exhaustiva.

Por tanto, el tratamiento de datos de salud y a gran escala entraría dentro de los supuestos en que es obligatorio realizar una EIPD. Sin embargo, en el caso que nos ocupa, no existe una EIPD realizada para los tratamientos de datos afectados por la brecha. El SESCAM Talavera justifica esta inexistencia en que se trata de sistemas de información implantados con anterioridad a la actual normativa de protección de datos (años 2005 y 2008).

A este respecto, en el citado documento (WP248, página 15, III.c) se señala lo siguiente:

<<*El requisito de realizar una EIPD se aplica a operaciones de tratamiento <u>existentes</u> que probablemente entrañan un alto riesgo para los derechos y libertades de las personas físicas y para las que se ha producido un cambio de los riesgos, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento. No será necesaria una EIPD para operaciones de tratamiento que hayan sido comprobadas por una autoridad de control o el delegado de protección de datos, de conformidad con el artículo 20 de la Directiva 95/46/CE, y que se realicen de una forma que no haya cambiado desde la anterior comprobación.*

En cambio, esto significa que deberán someterse a una EIPD los tratamientos cuyas condiciones de aplicación (alcance, fin, datos personales recogidos, identidad de los responsables o destinatarios del tratamiento, periodo de conservación de datos, medidas técnicas u organizativas, etc.) hayan cambiado desde la anterior comprobación realizada por la autoridad de control o el delegado de protección de datos y que probablemente entrañen un alto riesgo.

Además, podría requerirse una EIPD después de que se produzca un cambio de los riesgos a causa de las operaciones de tratamiento, por ejemplo, debido a la puesta en marcha de una nueva tecnología o a que los datos personales se usan para un fin distinto. Las operaciones de tratamiento de datos pueden evolucionar rápidamente y pueden surgir nuevas vulnerabilidades. Por tanto, cabe señalar que la revisión de una EIPD no resulta útil solo para la mejora continua, sino que también es fundamental para mantener el nivel de protección de datos en un entorno que evoluciona con el tiempo. Una EIPD también puede resultar necesaria debido a cambios en el contexto organizativo o social de la actividad de tratamiento, por ejemplo, debido a que los efectos de determinadas decisiones automatizadas hayan ganado importancia o a que

nuevas categorías de interesados se vuelvan vulnerables a la discriminación. Cada uno de estos ejemplos podría ser un elemento que originase un cambio del riesgo resultante de la actividad de tratamiento en cuestión.

En cambio, ciertos cambios también podrían reducir el riesgo. Por ejemplo, una operación de tratamiento podría evolucionar de forma que las decisiones ya no fueran automatizadas o una actividad de observación ya no fuera sistemática. En ese caso, la revisión del análisis de riesgo realizada puede mostrar que ya no se requiere la realización de una EIPD.

Por razón de buenas prácticas, una EIPD debe ser continuamente revisada y reevaluada con regularidad. Por tanto, incluso si el 25 de mayo de 2018 no se requiere una EIPD, será necesario, en el momento oportuno, que el responsable del tratamiento lleve a cabo una evaluación de este tipo como parte de sus obligaciones generales de responsabilidad proactiva.>>

El enfoque de riesgos que establece el RGPD supone que la EIPD debe entenderse como un proceso y no como un estado. Por lo tanto, si bien la EIPD se ha de realizar antes de la implementación del tratamiento, su revisión y adaptación se extiende a todas las etapas del ciclo de vida de este.

Como se señala en las citadas Directrices WP248, si durante la vida del tratamiento se producen cambios, como cambios contextuales o una ampliación no prevista del ámbito/alcance, será necesario actualizar la EIPD y, en su caso, generar un nuevo informe y plan de acción con las medidas de control adicionales que fuera necesario implantar en el marco de la gestión del riesgo antes de continuar con el tratamiento. Si no se hubiera realizado la EIPD porque las circunstancias iniciales no obligaban o no lo recomendaban, entonces sería necesario realizar la EIPD desde cero. En estos casos, la EIPD se ha de ejecutar de forma inmediata. (Guía de la AEPD *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, revisada en junio 2021)

Por lo tanto, es obligación del responsable realizar una revisión del nivel de riesgo en los tratamientos ya en curso de cara a determinar el momento oportuno para realizar la EIPD.

Teniendo en cuenta que en el momento de producirse la brecha ya han transcurrido más de tres años desde la plena entrada en vigor del RGPD y que los sistemas de información llevan, según el SESCAM muchos años implantados (2005, 2008), difícil resulta - por la potencial evolución en la naturaleza, el contexto e incluso alcance al que están sujetos los mismos- que no se hayan producido cambios en las condiciones del tratamiento (alcance, contexto, finalidades, funcionalidades, datos personales recogidos, identidad de los responsables o de los encargados, destinatarios, combinaciones de datos, riesgos, medidas de seguridad, período de conservación de los datos, sistemas de bloqueo, cambios jurídicos, medidas técnicas u organizativas, etc). A más, en la propia Auditoría realizada en 2018 expresamente se indica como una de las medidas correctivas la necesidad de realizar una evaluación del cumplimiento de estos sistemas a la actual normativa de protección de datos, evaluación que debe concluir con un plan de adecuación. Y se insiste, no debe olvidarse que se trata de un tratamiento a gran escala de datos de salud, tratamiento

de alto riesgo, para los que, de forma expresa el artículo 35.3 a) del RGPD obliga a realizar una EIPD. No llevar a cabo ninguna revisión o no realizar la EIPD de estos tratamientos *sine die*, no puede entenderse, en ningún caso, como una forma de demostrar el cumplimiento de lo previsto en el RGPD con relación al marco de responsabilidad proactiva.

En este sentido, el RGPD requiere que los responsables del tratamiento apliquen medidas adecuadas para garantizar y poder demostrar el cumplimiento de dicho reglamento, teniendo en cuenta entre otros, "*los riesgos de diversas probabilidad y gravedad para los derechos y libertades de las personas físicas*" (art. 24). Por tanto, la obligación de los responsables del tratamiento de llevar a cabo una EIPD en determinadas circunstancias debe entenderse en el contexto de su obligación general de gestionar adecuadamente los riesgos derivados del tratamiento de datos personales. Se trata de un enfoque basado en el riesgo y los responsables deben evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuándo es probable que un tipo de tratamiento *entrañe un alto riesgo para los derechos y libertades de las personas físicas*.

Por tanto, para gestionar estos riesgos, los mismos deben no sólo evaluarse (identificarse, analizarse, estimarse, tratarse (p.ej. mitigarse), sino también que dicha evaluación debe revisarse con regularidad. Es decir, dentro de la responsabilidad proactiva a que está sujeta el responsable del tratamiento, es obligación de este revisar y actualizar las medidas cuando sea necesario, por cuanto una EIPD no es un estado, sino que es un proceso.

Por tanto, confirmada la citada infracción del artículo 35 del RGPD, corresponde sancionar con un apercibimiento a SESCAM Talavera.

XIII
Tipificación de la infracción del artículo 35 del RGPD

La citada infracción del artículo 35 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4,*

5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes: (…)*

> *t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.*

XIV
Sanción por la infracción del artículo 35 del RGPD

Sin perjuicio de lo dispuesto en el artículo 83.4 del RGPD, el citado artículo dispone en su apartado 7 lo siguiente:

"7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro".

Por su parte, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que

no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo. (…)"

Por tanto, confirmada la citada infracción del artículo 35 del RGPD, corresponde sancionar con un apercibimiento a SESCAM Talavera

XV
Imposición de medidas

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

En concreto, si en la actualidad no se ha realizado aún, proceder a llevar a cabo las medidas pertinentes para solventar las deficiencias detectadas que han supuesto la vulneración del artículo 32 y puestas de manifiesto el Fundamento de Derecho VI de la presente Resolución, así como proceder a realizar la correspondiente EIPD respecto de los tratamientos de datos personales llevados a cabo por SESCAM Talavera como responsable y que estén sujetos a dicha obligación.

Se advierte que no atender la orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, una sanción de APERCIBIMIENTO.

SEGUNDO: IMPONER a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, por una infracción del Artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

TERCERO: IMPONER a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, por una infracción del Artículo 33 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

CUARTO: IMPONER a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, por una infracción del Artículo 35 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de APERCIBIMIENTO.

QUINTO: ORDENAR A SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, para que en el plazo de 6 meses:

- acredite la realización de las EIPD respecto de los tratamientos de datos personales sujetos a dicha obligación.

- acredite la implantación de las medidas pertinentes para solventar las deficiencias detectadas que han supuesto la vulneración del artículo 32 y puestas de manifiesto el Fundamento de Derecho VI de la presente Resolución.

SEXTO: PROPONER a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H, la iniciación de actuaciones disciplinarias contra las personas responsables de los accesos indebidos.

SÉPTIMO: DAR TRASLADO de la reclamación a la Fiscalía General del Estado para que analice la posible comisión de un ilícito penal.

OCTAVO: NOTIFICAR la presente resolución a SERVICIO DE SALUD CASTILLA MANCHA TALAVERA, con NIF Q4500146H

NOVENO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-180523

Mar España Martí
Directora de la Agencia Española de Protección de Datos