- **Procedimiento Nº: E/08945/2019**

940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad de datos personales remitido por la CONSEJERÍA DE SALUD Y FAMILIAS, con NIF Q5783675, de la JUNTA DE ANDALUCÍA, en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) que en el desarrollo de una nueva aplicación informática sobre gestión de formación sanitaria especializada de internos residentes, por error, se incluyó un antiguo fichero con datos reales de especialistas internos residentes que han sido expuestos al público a través de robots de búsqueda y junto con el código fuente de la aplicación.

SEGUNDO: La Subdirección General de Inspección de Datos procede a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación: 18 de septiembre de 2019

ENTIDADES INVESTIGADAS

CONSEJERÍA DE SALUD Y FAMILIAS, con NIF Q5783675, y dirección postal en Avenida de la Innovación s/n. Edificio Arena 1, 41020 Sevilla

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fechas 27 de septiembre y 19 de noviembre de 2019 se requiere información a la Consejería de Salud y Familias y de la respuesta recibida por parte de Fundación Pública Andaluza Progreso y Salud (NIF G41825811), en calidad de encargada del tratamiento y adscrita a la citada Consejería, se desprende lo siguiente:

Respecto de la empresa. Contratos empresas encargadas del tratamiento

- La Fundación Pública Andaluza Progreso y Salud (en adelante FPS) es una organización dependiente de la Consejería de Salud y Familias de la Junta de Andalucía que presta servicio al Sistema Sanitario Público Andaluz, tal y como figura en la web sspa.juntadeandalucia.es/fundacionprogresysalud/es.

- Hasta el año 2017, el Servicio Andaluz de Salud tenía encomendada la gestión de la formación de especialistas internos residentes (servicio *PORTALEIR*) que pasó a titularidad de la actual Secretaria General de Investigación, Desarrollo e Innovación de la Consejería de Salud y Familias. (cambio de titularidad publicada en el boletín Oficial de la Junta de Andalucía).

- En el año 2017, FPS, en calidad de encargado del tratamiento, comienza el desarrollo de un nuevo proyecto en el ámbito de la formación de los especialistas internos residentes que a su vez lo contrata con la entidad ISOTROL, S.A. (NIF A41142241, en adelante ISOTROL) actuando en calidad de subencargado del tratamiento.

FPS ha aportado copia del contrato suscrito con ISOTROL, adjudicataria de la convocatoria de 6 de abril de 2017 para el "*Servicio de soporte y desarrollo que permita la implantación de los procedimientos de gestión de la formación de especialistas en ciencias de la salud por medios electrónicos a través de la plataforma web PORTALEIR"* y Pliego de condiciones de la convocatoria donde consta como objeto del contrato *"el diseño, desarrollo, validación, pilotaje e implantación de nuevos módulos en la plataforma PORTALEIR".*

Asimismo, ha aportado Anexo al contrato en donde figura que la responsable del tratamiento es la Consejería de Salud y Familias asumiendo FPS la función de encargado del tratamiento, e ISOTROL la consideración de subencargado del tratamiento.

Respecto de la cronología de los hechos. Medidas de minimización de la incidencia

- El 17 de septiembre de 2019 a las 13:48 se tiene conocimiento de un incidente de seguridad en relación con los datos personales de internos residentes del sistema de información *PORTALEIR* comunicado por el Jefe de Servicio de Informática de la Consejería de Salud y Familias. Este incidente es registrado en el Sistema de Gestión de Incidentes de la entidad FPS.

En ese momento, se comprueba por FPS la publicación en Internet de datos personales de los especialistas internos residentes del año 2007 que figuraban en su plataforma de desarrollo.

FPS ha aportado impresiones de pantalla de evidencias sobre el incidente de seguridad de datos personales (nombre y apellidos, dirección de mail y teléfono).

- A las 13:55, FPS contacta con ISOTROL para informar de la incidencia y solicitan la resolución, que se lleva a cabo a las 16:01 eliminado la página publicada por error en Internet en la que constaba una versión del código fuente y datos sobre contactos de especialistas internos residentes del año 2007.

- A las 16:33 se comunica al DPD de la Consejería de Salud y Familias la solución una vez confirmada por FPS.

Respecto de las causas que hicieron posible la incidencia

- La incidencia fue causada al publicar en Internet, por parte de ISOTROL (subencargado del tratamiento) de una versión antigua del código fuente que contenía datos de carácter personal del personal en formación de especialistas internos residentes relativos al año 2007.

Respecto de los datos afectados. Notificación e indexación

- Los datos indebidamente publicados corresponden a: Nombre y apellidos, DNI y datos de contacto (dirección de mail y teléfono) del año 2007.

- El número aproximado de afectados es de 1000.

- FPS manifiesta que no se ha comunicado la incidencia a los posibles afectados.

- La Consejería no tiene constancia del acceso por terceros ajenos a estos datos, salvo el acceso por el ciudadano que comunicó la incidencia.

- La Consejería manifiesta que se realizaron comprobaciones en los buscadores de Internet y no mostraban los datos publicados.

Respecto de las acciones tomadas para la resolución final de la incidencia o para minimizar el impacto

- Se han tomado las medidas necesarias para eliminar en el código fuente de las versiones del aplicativo la inclusión de datos relativos a los especialistas internos residentes para evitar que pueda volver a suceder.

- FPS manifiesta que en los códigos fuentes del sistema ya no constan datos personales.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- FPS ha aportado copia del Registro de Actividades de Tratamiento (RAT) correspondiente al sistema de información PORTALEIR.

- Respecto del Análisis de Riesgos manifiestan que están trabajando en un proyecto de adaptación al Esquema Nacional de Seguridad. En este momento disponen del borrador del Análisis de Riesgo de los *Activos* basado en la herramienta <<*PILAR*>> entre los que se encuentra el sistema de información PORTALEIR.

A este respecto, han aportado copia del mencionado proyecto de fecha 15 de enero de 2020.

- FPS ha aportado copia del procedimiento sobre *gestión de incidencias* en el que se contempla el procedimiento de notificación de brechas de seguridad.

- FPS está incluida en el ámbito de aplicación de la Política de Seguridad de la Consejería y aportan, entre otros, los siguientes documentos:

    o Política de Seguridad TIC de la Consejería.

    o Resolución de 13 de julio de 2018 de la Dirección General de Telecomunicaciones y Sociedad de la Información de la Junta de Andalucía por la que se establecen las normas de gestión de incidentes de seguridad.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra 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."*

El artículo 33 del RGPD señala lo siguiente:

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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."

En el presente caso, consta una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, como consecuencia de la publicación indebida en Internet por la Consejería de Salud y Familias de la Junta de Andalucía de datos personales de los especialistas internos residentes correspondientes al año 2007, y que ha tenido su origen en la realización de pruebas en el sistema de información con datos reales sin haber considerado adecuadamente el riesgo y posible impacto que implica.

De las actuaciones de investigación se desprende que la Consejería de Salud y Familias, en calidad de responsable del tratamiento, disponía de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, también disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación del incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de corregir, notificar, minimizar el impacto e implementar nuevas medidas razonables y oportunas para evitar que se repita en el futuro la incidencia a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas, como son el responsable del tratamiento, encargado y subencargado del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de personas afectadas como consecuencia del incidente.

En consecuencia, consta que la Consejería de Salud y Familias en calidad de responsable del tratamiento, disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo evaluado para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la ahora analizada.

III

Por lo tanto, se ha acreditado que la actuación de la Consejería de Salud y Familias en calidad de responsable del tratamiento, ha sido proporcionada y acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a CONSEJERÍA DE SALUD Y FAMILIAS, con NIF Q5783675 y dirección postal en Avenida de la Innovación s/n. Edificio Arena 1, 41020 Sevilla.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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