- **Procedimiento Nº: E/01364/2020**

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: Con fecha de 10 de febrero de 2020, la Directora de la Agencia Española de Protección de Datos (en adelante, AEPD) acuerda el inicio de actuaciones de investigación en relación a una brecha de seguridad de datos personales notificada por el SERVICIO CANARIO DE LA SALUD (en adelante SCS) en fecha 03 de febrero de 2020, relativa al fallo en aplicación informática que supuso el acceso indebido al informe clínico de un tercero.

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

ENTIDADES INVESTIGADAS

SERVICIO CANARIO DE LA SALUD, con NIF Q8555011I y domicilio en Avenida Juan XXIII, 17, Planta 6ª, 35071 Las Palmas de Gran Canaria (Las Palmas).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Respecto a los hechos:

- El SCS dispone de una aplicación informática denominada "******APLICACIÓN.1***", accesible por web y por *app* móvil, en la que cada paciente puede acceder a su historia clínica de manera digital. El SCS informa de que dicha aplicación informática almacena registros con información de los informes clínicos existentes, incluyendo información demográfica del paciente titular y un número de referencia con el que puede accederse al informe disponible en el servicio informático del Hospital que lo custodia

- El 29 de enero de 2020, el SCS manifiesta haber recibido comunicación telefónica de un ciudadano que en el acceso por *app* móvil a su historia clínica en "******APLICACIÓN.1***" obtiene el informe clínico de laboratorio de otro paciente.

- El SCS declara que, tras comprobarse el acontecimiento de la brecha de seguridad, se cerró el acceso al repositorio de historias clínicas "******APLICACIÓN.1***" en la web y en la *app* móvil.

- Siete horas después del incidente, el SCS expone haber identificado que el problema corresponde a analíticas de un hospital adscrito al SCS, debido a una reutilización de número de referencia de informes en su sistema de información de laboratorio (en adelante, LIS) que provoca en el repositorio una incorrecta asociación paciente-informe. De acuerdo con esta identificación del origen del incidente, el SCS manifiesta haber reestablecido el acceso en "******APLICACIÓN.1***" a todos los informes clínicos salvo a las analíticas del hospital afectado.

- El 3 de febrero de 2020, el SCS expresa que confirmó el incidente con el usuario que detectó la brecha de seguridad. En primera instancia, el SCS expuso haberle solicitado a dicho paciente que suprimiese la información obtenida indebidamente.

- Entre la anterior fecha y el 18 de febrero de 2020, el SCS manifiesta haber desempeñado tareas conjuntas con el hospital afectado para determinar el alcance de la brecha de seguridad en cuestión. Ese mismo día, el SCS enuncia haber concluido los trabajos de determinación del alcance de la brecha de seguridad de manera que se pasan a identificar los siguientes:

    - 122 accesos indebidos de 34 usuarios a resultados de analíticas de 45 pacientes, de los cuales 3 son fallecidos, del hospital afectado.

- El SCS informa de que los citados trabajos de subsanación consistieron en el cruce de información de números de referencia que habían sido reutilizados por el LIS del hospital afectado con los datos demográficos de usuarios (susceptibles de estar erróneamente vinculados), exponiendo haber comprobado posteriormente si en cada caso existió un acceso indebido.

- El SCS declara que la incorrecta asignación informe-paciente se produce por el desbordamiento del contador del LIS del hospital afectado, derivando en la reseñada errónea reutilización del número de referencia.

- El SCS manifiesta no tener constancia de uso por terceros de los datos personales accedidos en la brecha de seguridad investigada.

- El SCS señala que el tratamiento de los datos comprometidos en la brecha de seguridad alcanza en "******APLICACIÓN.1***" a las actividades de tratamiento de Tarjeta Sanitaria Individual, de Historia Clínica de Atención Primaria y de Historia Clínica de Atención Especializada.

2. Respecto a las medidas previas al acontecimiento de la brecha de seguridad:

- El SCS declara disponer de la opción de paso a producción mediante procesos automatizados de nuevas versiones de sus aplicaciones informáticas y de un "botón de pánico" a disposición de los responsables de informática para una suspensión inmediata del servicio que dichas aplicaciones proveen.

- El SCS aporta la <*Resolución de 11 de diciembre de 2018, del Director del SCS, por la que se registran determinadas actividades de tratamiento de datos personales*> en la que se reconocen, entre otras, las siguientes actividades de tratamiento de datos personales relativas a:

    - Tarjeta Sanitaria Individual

    - Historia Clínica de Atención Primaria

    - Historia Clínica de Atención Especializada

  Asimismo, se incorporan los correspondientes documentos de información RAT (registro de actividades de tratamiento), en los que se identifican los términos en que el SCS es el responsable del tratamiento de los datos de las tres actividades señaladas.

- El SCS aporta un AR (análisis de riesgos) asociado al tratamiento de datos que realiza, presuntamente en 2017, en el que se estiman los siguientes riesgos asociados a las tres actividades de tratamiento en cuestión:

    - Tarjeta Sanitaria Individual: riesgo crítico, derivado de un impacto de las amenazas evaluado como muy alto y de una probabilidad de materialización de las amenazas evaluada como media.

    - Historia Clínica de Atención Primaria: riesgo crítico, derivado de un impacto de las amenazas evaluado como muy alto y de una probabilidad de materialización de las amenazas evaluada como media.

    - Historia Clínica de Atención Especializada: riesgo crítico, derivado de un impacto de las amenazas evaluado como muy alto y de una probabilidad de materialización de las amenazas evaluada como media.

- El SCS no ha realizado EIPD (evaluación de impacto relativa a la protección de datos) asociado a los riesgos anteriores de cada una de las tres actividades de tratamiento señaladas. El SCS alega que esta decisión fue tomada en su Comité de Seguridad de 24 de abril de 2018 y que se fundamenta, literalmente, en:

"ser tratamientos anteriores a la entrada en vigor del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE".

- El SCS evidencia disponer de dos modelos de comunicación a afectados por brechas de seguridad en los términos ocurridos en la investigada. En detalle, uno de los modelos correspondería al envío a pacientes que acceden indebidamente a informes de historia clínica digital de terceros y el otro al envío a pacientes a los que se les notifica que un tercero ha accedido indebidamente a su historia clínica digital. El SCS manifiesta no haber realizado esta comunicación a los afectados por la brecha de seguridad investigada, aunque sí señaló en la notificación de la brecha de seguridad que los interesados serían contactados en este sentido.

- El SCS aporta la <*Resolución de 5 de febrero de 2014, de la Directora del Servicio Canario de la Salud, por la que se aprueba la Política de Seguridad de la Información*> (Boletín Oficial de Canarias de 13 de febrero de 2014), en la que informa haber desarrollado la citada política de seguridad de la información del SCS de acuerdo a los principios del ENS (esquema nacional de seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito del régimen jurídico del sector público, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada).

- El SCS manifiesta estar informado en la plataforma tecnológica INES (iniciativa española de *software* y servicios, que constituye una red de cooperación científico-tecnológica integrada por los agentes tecnológicos relevantes del área) del grado de implantación de las medidas de seguridad del ENS.

3. Respecto a las medidas posteriores al acontecimiento de la brecha de seguridad:

3.1. De carácter correctivo (reactivas para subsanar la brecha de seguridad):

- El SCS expone haber interrumpido el acceso completo a informes de analíticas en "******APLICACIÓN.1***" desde que confirmó la existencia de la presente brecha de seguridad. A 28 de febrero de 2020, el SCS informa que la citada paralización de acceso en "******APLICACIÓN.1***" se mantenía vigente para los informes de laboratorio del hospital afectado, manifestando haber comprobado que la causa de la brecha de seguridad en cuestión no se produce en ningún otro sistema que almacene informes clínicos.

3.2. De carácter preventivo (proactivas para evitar que se repita la brecha de seguridad):

- El SCS declara haber acordado la ampliación del tamaño del campo identificador en el número de referencia de "******APLICACIÓN.1***" para concatenarlo a la fecha del informe. Con ello, el SCS dice pretender garantizar la correcta asignación paciente-informe en la aplicación informática, especialmente ante potencial desbordamiento del contador de la misma, pues incorpora otro campo más, el de la fecha, con el que detectar el error.

- El SCS manifiesta realizar una limpieza completa del repositorio centralizado de los números de referencia en "******APLICACIÓN.1***", con la pretensión de evitar duplicidades, así como de ajustar el número de referencia de los informes existentes y bloqueados a la nueva nomenclatura con la fecha incorporada.

- El SCS expone tener previsto terminar la implantación total de las medidas preventivas en "******APLICACIÓN.1"*** antes del 27 de marzo de 2020.

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 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 que se produjo una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso, a través del sitio web "******APLICACIÓN.1***" del SCS, a datos de terceros ajenos.

No obstante, también consta que el SCS a través del servicio de Informática, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora

analizado, lo que ha permitido tras una reclamación de un ciudadano la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorase la adopción de medidas técnicas y de gestión, como son las medidas preventivas y de acción rápida, al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

No constan reclamaciones ante esta AEPD por los afectados.

Por último, cabe señalar que consta aportada por el SCS <*Resolución de 5 de febrero de 2014, de la Directora del Servicio Canario de la Salud, por la que se aprueba la Política de Seguridad de la Información*> en la que se desarrolla la política de seguridad de la información del SCS de acuerdo a los principios del ENS, y estar informado en la plataforma tecnológica INES del grado de implantación de las medidas de seguridad del ENS.

Por último, se recomienda elaborar un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. 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 analizada.

III

Por lo tanto, la actuación del reclamado como entidad responsable del tratamiento ha sido diligente y proporcionada 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 la DIRECCION SERVICIO CANARIO DE LA SALUD con NIF Q8555011I y con domicilio en AVENIDA JUAN XXIII, NUM 17, PISO 6 - 35004 LAS PALMAS DE GRAN CANARIA (LAS PALMAS)

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