**Procedimiento Nº: E/07026/2019**
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 remitido por el Servicio Canario de Salud (en adelante SCS) en el que informan a la Agencia Española de Protección de Datos que tras el despliegue de una versión de un servicio de integración de datos, los usuarios que consultaron el listado de informes y analíticas a través de historia web, obtenían el listado de informes disponibles para un "paciente ficticio" entre los cuales se incluían 11 informes de laboratorio que correspondían respectivamente a 11 pacientes reales.
El total de usuarios de la aplicación web que accedieron a dichos informes es de 22. El número de accesos que se realizaron a estos informes es de 64. el periodo temporal de vulnerabilidad del sistema fue entre las 9:05 y las 11:55. no se vieron afectados otros servicios de acceso a la historia clínica ni otros informes distintos a los 11 citados

**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 reclamación, teniendo conocimiento de los siguientes extremos:

### ANTECEDENTES

Fecha de notificación de quiebra: 28 de junio de 2019.

### ENTIDADES INVESTIGADAS

***DIRECCION SERVICIO CANARIO DE LA SALUD con NIF Q8555011I con domicilio en AVENIDA JUAN XXIII, NUM 17, PISO 6 - 35004 LAS PALMAS DE GRAN CANARIA (LAS PALMAS)***

### RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1 Con fecha 31 de julio de 2019 se solicita por la inspección de datos información al Servicio Canario de Salud en relación con la incidencia de seguridad comunicada, teniendo entrada con fecha 23 de agosto de 2019 escrito de dicho responsable en el que pone de manifiesto lo siguiente:

1.1. Respecto a las causas y condiciones que se dieron para que se produjera la incidencia:

La primera de ellas fue la realización de un despliegue programado en la plataforma de integración que incluían mejoras en el servicio digital de ******URL.1***. Este despliegue contenía un error que redirigía a todos los ciudadanos conectados a ******URL.1*** al paciente ficticio. El error citado sólo afectó a uno de los canales de acceso, el canal web, del servicio digital

***URL.1**. Esta circunstancia se dio al pasar el plan de pruebas previsto sólo en el canal móvil y no en el canal web.

La segunda circunstancia es que dicho paciente ficticio tenía asociados 11 informes de laboratorio que correspondían a pacientes reales. El paciente ficticio es un paciente utilizado para la realización de pruebas de los sistemas para asegurar que los despliegues en cada uno de los entornos son correctos y el funcionamiento es el esperado. Este paciente existe en los diferentes entornos por el cual van pasando todos los sistemas para ser probados antes de su puesta en producción.

1.2. Una vez detectada la incidencia se tomó una única medida para minimizar el impacto de la incidencia. El 26 de junio a las 11:55 queda detenido el servicio web utilizado por los servicios digitales, en el que se incluye ***URL.1**, para impedir el acceso al sistema por parte de los ciudadanos. Desde ese momento, la incidencia de seguridad queda neutralizada y se comienzan con las acciones para restablecer el servicio de forma adecuada siendo el periodo de incidencia desde las 9:05 hasta las 11:55 de ese mismo día.

1.3. Para subsanar la incidencia, entre las 11:55 y las 12:30, se realizaron las siguientes acciones:

Analizar la causa de la incidencia y determinar los servicios que pudieran verse impactados. Detectando la incidencia descrita en el canal web del servicio digital de ***URL.1** así como la información incorrecta asociada al paciente ficticio.

Se procede a eliminar los informes identificados como "informes no de pruebas" del paciente ficticio en todos los entornos existentes quedando eliminados los 11 informes comentados.

Se procede a corregir la re-dirección al paciente ficticio para el canal web del servicio digital de ***URL.1** y se comienza con el protocolo de puesta en producción del servicio y la activación del mismo de cara a la ciudadanía.

Se realiza análisis del impacto de confidencialidad de la brecha de seguridad. Se identifican los pacientes afectados, los informes y los usuarios que acceden durante la brecha a los efectos de preparar las comunicaciones de violación de seguridad de datos personales y la notificación del incidente a la autoridad de control (AEPD).

Sobre los informes, la Dirección General de Programas Asistenciales estudia el grado de impacto en la confidencialidad de la información comprometida, concluyendo que los informes son pruebas de laboratorio, en algunos casos de fallecidos, y que no muestran resultados relevantes desde el punto clínico.

El tiempo de parada del servicio fue de 35 minutos desde la detección de la incidencia hasta restablecer completamente el servicio de cara a la ciudadanía.

1.4. No les consta el tratamiento posterior de los datos comprometidos. No obstante, a los 22 usuarios que accedieron a informes visibles durante la brecha se les remitió por correo postal una carta explicativa del incidente y en la que se le advertía al usuario que *"... Tras estas actuaciones, le pedimos disculpas y le recordamos que la difusión de datos personales que afecten a*

*la intimidad de otras personas está prohibido por la Ley, por lo que en caso de haber descargado la documentación visualizada o haberla impreso debe proceder a su destrucción si todavía no lo ha hecho y no comunicar a nadie los datos que figuran en los informes accedidos. ...".*

1.5. La aplicación que generó la brecha de seguridad trata datos de tres registros de actividad de tratamiento: Tarjeta Sanitaria, Historia Clínica de Atención Primaria e Historia Clínica de Atención Especializada. Aportan las resoluciones por las que se registran los citados tratamientos y sus respectivos documentos de información adicional.

1.6. Aportan el último Análisis de Riesgos realizado. Respecto a evaluaciones de impacto no se han realizado por tratarse de un tratamiento anterior a la entrada en vigor del Reglamento Europeo de Protección de Datos conforme a la decisión al respecto tomada en el pasado Comité de Seguridad de fecha 24 de abril de 2018.

1.7. Aportan copia del procedimiento establecido para tratar las brechas de seguridad tras la entrada en vigor del Reglamento Europeo de Protección de Datos.

1.8. Aportan copia de la Política de Seguridad del SCS publicada en la sede electrónica. Adicionalmente respecto a medidas concretas para mitigar posibles incidentes de la misma naturaleza, se han aplicado las siguientes medidas:

- Medida preventiva de auditoría continua de pacientes ficticios
- Medida preventiva de paso a producción de nuevas versiones mediante procesos automatizados.
- Medida preventiva de doble comprobación de la identidad del ciudadano a la hora de mostrarle informes.
- Medida correctora de disponibilidad de un "botón do pánico" a disposición de los responsables de informática para una suspensión inmediata del servicio dado.

## 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."

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso, a través del sitio web ******URL.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 es la contratación de una auditoria continua a todos los sistemas de información similares y otras 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.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

**III**

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido 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 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