- **Procedimiento Nº: E/08081/2020**

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 25/09/2020, la entidad BIOTRONIK SPAIN SA, con NIF A28985034 (en adelante, Biotronik), notificó -con número de registro de entrada O00007128e2000003249 - a la División de Innovación Tecnológica de esta Agencia una brecha de seguridad de datos personales, en relación con el acceso indebido a datos personales de pacientes erróneos, en los siguientes términos:

Durante una operación de mantenimiento de los sistemas de información de la matriz de BIOTRONIK SPAIN SA datos de pacientes registrados en el sistema *Home Monitoring Service Center* (HMSC) fueron visibles por otros profesionales sanitarios sin autorización para consultar esa información.

Los datos comprometidos fueron los básicos, de contacto y de salud de unas ocho personas pudiendo haber afectados también en Alemania.

Han comunicado la brecha a los afectados.

Han aportado escritos en relación con la comunicación a los afectados y listados de responsables de tratamiento posibles afectados por la brecha en el que figuran ocho hospitales españoles.

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:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

BIOTRONIK SPAIN SA, con NIF A28985034, y con domicilio en Avd. EUROPA, 19 - EDIFICIO III. 3ª PLANTA - 28224 POZUELO DE ALARCÓN (MADRID).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 27 de octubre de 2020 se solicitó información a BIOTRONIK SPAIN, S,A.. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- Tal y como consta en la web https://www.biotronik.com/es-es, BIOTRONIK forma parte del grupo BIOTRONIK SE & Co.KG, cuya sede se encuentra ubicada en Berlín (Alemania), empresa de ámbito mundial de dispositivos

médicos que dispone de productos y servicios para enfermedades cardiovasculares y endovasculares.

- BIOTRONIK Home Monitoring usa una tecnología telemédica para monitorizar el estado cardiaco de pacientes que tienen marcapasos y monitores cardiacos. Proporciona información de terapia y de diagnóstico de los pacientes entre las consultas de seguimiento programadas.

  El transmisor recibe los datos que le envía el dispositivo y los transmite al Centro de Servicio de BIOTRONIK a través de la red de telefonía móvil.

  El Centro de Servicio de BIOTRONIK recibe los datos enviados por el transmisor y los evalúa. Los resultados de la evaluación se ponen a disposición en informes y de forma resumida en la plataforma segura de Internet denominada BIOTRONIK Home Monitoring Service Center (HMSC). En la vista pormenorizada se dispone del historial médico de cada paciente y los detalles del informe actual.

  Se ha aportado Manual técnico del del Sistema Home Monitoring.

- BIOTRONIK tiene definidos los compromisos de confidencialidad en el documento "*Términos de Uso para el Sistema BIOTRONIK Home Monitoring System y ReportShare*" (apartado Cumplimiento legal y consentimiento del paciente) que los usuarios del sistema (profesionales sanitarios médicos) aceptan expresamente cuando acceden al mismo, sin perjuicio de que los Hospitales, como responsables del tratamiento, dispongan de un compromiso de confidencialidad propio con sus profesionales médicos. Adicionalmente, cabe destacar que todos los usuarios son facultativos médicos sujetos a código deontológico corporativo, que incluye, entre otros, la obligación de secreto en telemedicina. Han aportado el documento "*Términos de Uso para el Sistema BIOTRONIK Home Monitoring System y ReportShare"*

<u>Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final</u>

BIOTRONIK ha aportado informe de resolución de brecha de confidencialidad en el que consta:

- El día 22 de septiembre de 2020 BIOTRONIK recibió una alerta de seguridad vía email desde la empresa matriz informando de que se ha visto afectado el servicio Home Monitoring Service Center (HMSC) provocado por un fallo de un software externo de mantenimiento de HSMC y se han visto afectados cuatro hospitales españoles.

  El incidente ha provocado que cierta información de pacientes haya sido visible para otros médicos o facultativos del servicio HSMC que no tenían autorización para el acceso a esta información.

- Inmediatamente después de detectar el incidente, la matriz de BIOTRONIK restringió el acceso de usuarios a la web del HMSC hasta que pudiera solucionarse la incidencia. Posteriormente se llevó a cabo un exhaustivo chequeo y se corrigió el problema.

- Los datos de pacientes pueden haber estado visibles durante un breve período de tiempo durante una sesión de usuario aislada, aunque no disponen de información sobre si dichos médicos accedieron realmente a la información.

  Los datos afectados corresponden con datos de contacto, datos de salud, nombre del médico, identificación del paciente, tipo de dispositivo/número de serie, fecha de implantación y datos médicos relacionados con el paciente.

- En relación con las medidas implantadas para mitigar el incidente

  BIOTRONIK manifiesta que la empresa matriz en Berlín al detectar el problema el miércoles 16 de septiembre a las 10 a.m. procedió a la desconexión del sitio web de HMSC con objeto de realizar un análisis y se volvió a conectar a las 12 p.m. una vez comprobado que un componente no funcionaba correctamente.

  El 17 de septiembre a las 8 p.m. el monitoreo detectó el comportamiento erróneo nuevamente y las salvaguardas implementadas desconectaron automáticamente el servicio como mecanismo de seguridad.

  Después de reemplazar completamente los componentes erróneos, el servicio volvió a estar en línea el 18 de septiembre a las 12:45 a.m. y tras la resolución de los problemas detectados el sistema volvió a funcionar de forma segura.

  BIOTRONIK manifiesta que la incidencia está resuelta y cerrada. Permanece un canal de comunicación abierto para respuestas a la AEPD y a los médicos y Delegados de Protección de Datos de Hospitales afectados. También, el día 25 de Septiembre, se ha informado a la red de ventas y técnicos para dar respuesta a cualquier cuestión que los médicos usuarios afectados o no afectados pudieran plantear.

- Además, se procedió a la comunicación a los hospitales afectados.

Se adjunta parte de incidencia y quejas e informe de resolución de brecha de confidencialidad.

Respecto de las causas que hicieron posible la brecha

- El error fue causado por un componente de un software de terceros que no trabajó como estaba planificado. Este error no era previsible y fue detectado tras un análisis programado del mantenimiento del sistema y posteriormente con una monitorización y análisis específico del problema.

Respecto de los datos afectados.

- Han sido afectados los siguientes hospitales:

- Clínico Universitario de Valencia,
- General Universitario de Alicante,
- OSI Araba
- Virgen de la Victoria

- Número de personas afectadas cinco

- Los datos corresponden con datos de contacto y de salud del paciente, nombre del médico, tipo de dispositivo/número de serie, fecha de implantación y datos médicos relacionados con el paciente.

- Un médico usuario pudo haber visualizado datos personales de un paciente no asignado. No se han podido editar ni borrar tales datos.

- BIOTRONIK solo puede identificar los potenciales usuarios que han tenido posible acceso (visualización de datos) y la tipología de datos que han podido ser visibles, no su utilización por terceros. Se ha comunicado la incidencia a los responsables del tratamiento y a los propios usuarios (profesionales sanitarios médicos).

  BIOTRONIK ha aportado dichas comunicaciones donde figura información sobre la incidencia y la solución que han implantado.

- BIOTRONIK no tiene acceso a los datos personales incluidos en el sistema. No obstante, el profesional médico no debe publicar en Internet, ni divulgar a terceros los datos de pacientes incluidos en el HMSC con base en sus obligaciones de confidencialidad y código deontológico corporativo.

<u>Respecto de las medidas de seguridad implantadas</u>

- El mantenimiento del HMSC se realiza únicamente de forma interna por la empresa matriz.

- BIOTRONIK tiene definidas las medidas técnicas y organizativas que protegen la transferencia y el procesamiento de los datos del sistema HMSC. Han aportado un documento al respecto.

- BIOTRONIK utiliza una plataforma para registrar la actividad de tratamiento de datos.

- Se ha aportado los siguientes documentos:

    - Registro de actividad para Home Monitoring.

    - Política de Seguridad.

    - Tratamiento de quejas e incidencias.

    - Informe de auditoría de seguridad.

    - Lista de medidas técnicas y organizativas generales en el sentido del art. 32 del RGPD de BIOTRONIK SE & CO. KG y medidas especiales relacionadas con el funcionamiento del Home Monitoring Service Center".

    - Procedimiento de Análisis de Riesgos y Análisis de Riesgos del software.

    - Evaluación de impacto de los tratamientos de datos personales que se realiza para la empresa BIOTRONIK conforme al reglamento general de protección de datos.

- Desde la detección de la brecha de confidencialidad, la empresa central ha añadido herramientas de monitorización para fortalecer el uso seguro del HMSC.

- Con posterioridad a la brecha se va a implantar un procedimiento específico de respuesta ante ciberincidencias.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

La incidencia ha sido aislada y ha ocurrido una única vez durante un periodo de tiempo limitado y no es recurrente.

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"* 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 art. 32 del RGPD, señala lo siguiente:

<<Artículo 32 Seguridad del tratamiento

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 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.>>.

III

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 del supuesto acceso indebido al contenido del sistema *Home Monitoring Service Center* del que Biotronik Spain S.A. es responsable.

De las actuaciones de investigación se desprende que la entidad Biotronik disponía con anterioridad a la incidencia de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, la entidad Biotronik 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 notificar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la supuesta incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el propio responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de personas afectadas.

En consecuencia, consta que la entidad Biotronik, en calidad de responsable del tratamiento afectado por la brecha de seguridad, disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo 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.

En el supuesto objeto de este procedimiento, se considera que se han tomado las medidas adecuadas para evitar que se vuelva a producir el incidente de seguridad referido, por lo que no se requiere al responsable de la adopción de nuevas medidas.

IV

Por lo tanto, se ha acreditado que la actuación del responsable del tratamiento ha sido diligente 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 BIOTRONIK SPAIN SA, con NIF A28985034, y con domicilio en Avd. EUROPA, 19 - EDIFICIO III. 3ª PLANTA - 28224 POZUELO DE ALARCÓN (MADRID).

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.

940-0419

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