- **Procedimiento Nº: E/01783/2020**

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: Con fecha de 25 de febrero de 2020 la directora de la Agencia Española de Protección de Datos (en adelante AEPD) acuerda iniciar actuaciones de investigación en relación con una brecha de seguridad de los datos personales notificada por TORREJÓN SALUD, S.A., relativa a un virus informático del tipo *ransomware* con afectación a la infraestructura de sus sistemas informáticos y disponibilidad de los datos personales.

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:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad: 20/01/2020

ENTIDADES INVESTIGADAS

TORREJON SALUD, S.A. (en adelante TS) con NIF A85740595 y domicilio en Calle Mateo Inurria S/N, 28850 Torrejón de Ardoz, Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Respecto a los hechos:

- TS manifiesta ser una entidad privada que gestiona por concesión administrativa el Hospital Universitario de Torrejón, sito en Torrejón de Ardoz (Madrid), el cual es un hospital público que forma parte de la red sanitaria del SERMAS (Servicio Madrileño de Salud, NIF: Q2801221I), adscrito a la Consejería de Sanidad de la Comunidad de Madrid. Se aporta un contrato, de fecha 10 de agosto de 2011, entre TS y el SERMAS en el que se estipula la cesión de datos del SERMAS a TS, así como los compromisos que TS adquiere como encargado de tratamiento de los datos de salud que le competen en su gestión del hospital.

Asimismo, TS evidencia la solicitud autorizada, con fecha 15 de septiembre de 2011, a la Dirección General de Hospitales de la Consejería de Sanidad de la Comunidad de Madrid, para que le sean cedidos los datos de historia clínica de sus pacientes según corresponde.

- TS expresa que el 17 de enero de 2020 sufrió un ataque de *ransomware* (secuestro de datos en el que un programa informático restringe la disponibilidad a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de eliminar dicha restricción), causando una indisponibilidad de los servicios TIC al cifrarse ficheros y dispositivos tanto de servidores como de puestos de usuario.

- TS declara que, en torno a las 16:00 horas del citado día, su personal de tecnologías de la información confirma, tras recibir aviso de malfuncionamiento en varios equipos, que el fallo es generalizado, encontrando evidencias de que puede tratarse de un ataque de *ransomware*.

- TS expone que tras unas actuaciones iniciales por parte del personal técnico informático en ese mismo día logra contener el incidente, evitando la propagación del *ransomware* a otras partes del sistema de información. Asimismo, TS expresa que al comienzo de la noche de la reseñada fecha ya se pone en marcha el plan de contingencia previsto para los días naturales siguientes (fin de semana).

- TS informa de que el día 18 de enero de 2020 se mantuvo en el propio Hospital Universitario de Torrejón una reunión con los responsables en materia de protección de datos y seguridad de la información de la Consejería de Sanidad de la Comunidad de Madrid. Según indica TS en esa reunión se dio conocimiento del estado de situación y acciones conjuntas a realizar respecto al *ransomware* detectado en su sistema de información.

- TS prueba que el día 19 de enero de 2020 notificó el presente incidente de seguridad de la información al CCN (centro criptológico nacional, organismo adscrito al Centro Nacional de Inteligencia).

- TS menciona haber continuado con labores de recuperación de sistemas afectados y con la ejecución del plan de contingencia los días 20 y 21 de enero de 2020.

- TS evidencia haber comparecido en las dependencias oficiales del Departamento de Delitos Telemáticos de la Guardia Civil en Madrid, a las 13:00 horas del día 22 de enero de 2020, para presentar denuncia sobre los hechos acontecidos como consecuencia de esta brecha de seguridad.

- TS dispone de un informe forense sobre la brecha de seguridad, elaborado por parte de consultora especializada (S2 Grupo) que en lo relativo a protección de datos concluye literalmente:

  - *La infección se inicia a través de un incidente de malware no detectado (probablemente espécimen Emotet) que da acceso a un equipo.*

  - *Logran credenciales para poder realizar movimiento lateral y alcanzar al controlador de dominio (Equipo desde el que ya se pueden realizar configuraciones sobre todo el parque de equipos de un dominio).*

  - *Se establecen políticas de configuración que reducen las medidas de seguridad ya aplicadas para lograr tener éxito en la distribución del malware que iba a utilizarse en una segunda fase.*

  - *Posteriormente, se distribuye el programa malicioso y se configuran los equipos para dar órdenes de ejecución produciéndose así la infección masiva.*

  - *Precisamente, en fecha 5 de marzo 2020, Microsoft ha publicado cuál es la estrategia que sigue este tipo de ataque, (puede verse a través de esta url:* ******URL.1***

- TS afirma no tener evidencias de que a partir del ataque con *ransomware* se haya accedido por terceros a datos personales e información contenida de los servidores.

- TS concluye que la tipología de los datos afectados es la siguiente:

  - Datos de carácter identificativo: DNI, dirección postal, dirección de correo electrónico, teléfono, CIPA, HCA.

  - Circunstancias sociales.

  - Características personales: sexo, año nacimiento.

  - Categorías especiales de datos: salud, Religión, Ideología, Creencias, Vida Sexual, Origen racial o étnico, Violencia de género, datos genéticos.

  - Categoría de interesados afectados: pacientes.

- TS estima el número de afectados en unas 200 personas, informando de que el Hospital Universitario de Torrejón tiene asignado en torno a 153.000 pacientes.

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

- TS presenta un RAT (registro de actividades de tratamiento), entre las que señala las siguientes como comprometidas en la presente brecha de seguridad:
    - Gestión en el registro de dispensa de estupefacientes.
    - Gestión de dispensación farmacéutica (pacientes internos).
    - Gestión de dispensación farmacéutica (pacientes externos).
    - Gestión clínico asistencial.
    - Gestión de CMDB (conjunto mínimo básico de datos).
    - Estadísticas y explotación de datos.
- TS aporta un conjunto documental de análisis de riesgos, en donde se incluye:
    - Metodología utilizada para la realización del análisis de riesgos.
    - Identificación y valoración de las amenazas.
    - Tratamiento del riesgo.
- TS documenta una EIPD (evaluación de impacto en protección de datos) en la que se concluye que el riesgo final asociado a los tratamientos que realiza es aceptable.
- TS resalta como defensas implantadas en su organización:
    - Adecuación al *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* (en adelante RGPD).

- Plan de Adecuación al ENS (esquema nacional de seguridad).

- Auditoría de medición del nivel de madurez del *framework* de seguridad NIST (*National Institute of Standards and Technology*).

- Auditoría y medición de acceso a historias clínicas del CPD (centro de procesamiento de datos) y de penetración a los sistemas del Hospital Universitario de Torrejón por parte del SERMAS.

- Elementos de *Governance* y ciberseguridad en materias diversas.

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):

- TS señala haber contemplado las siguientes:

  - Preparación de infraestructuras.

  - Saneamiento y restructuración del CPD.

  - Disponibilidad de infraestructura de contingencia (4 servidores, 1 cabina).

  - Disponibilidad de infraestructura base (24 Servidores físicos, 4 cabinas).

  - Existencia de infraestructuras de alta disponibilidad (3 clúster de virtualización, 3 clúster de BBDD)

  - Existencia de infraestructura de *backup* y de monitorización.

  - Disponibilidad de 300 equipos W10, bastionados y con acceso RDS (servicios de escritorio remoto) a granja *Terminal Server* para acceso general a historia clínica.

- TS alega no haber comunicado a los pacientes afectados la brecha de seguridad por, según expone, no haberse materializado daño alguno respecto a sus derechos y libertades, puesto que establece que la confidencialidad de sus datos no se vio comprometida y se garantizó en todo momento la continuidad asistencial.

Asimismo, TS remarca que sólo se vio afectada temporalmente la disponibilidad de la información por un periodo de tiempo reducido, y con un número potencial de personas afectadas no significativo respecto de la totalidad a los que ofrece servicio sanitario.

TS presenta un sucinto análisis del riesgo referido a la necesidad de comunicar a los afectados en el que se obtiene un resultado medio, y por ello, refiriéndose al artículo 34 del RGPD, exponen la no necesidad de proceder a comunicar la brecha de seguridad a los afectados.

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

- TS manifiesta que, a día 12 de marzo de 2020, se encontraban aun llevando a cabo tareas que prevendrían la reaparición de una brecha de seguridad como la que se produjo, en concreto:

  - Plan de proyectos en ejecución:

    - Migración Dominio.
    - Migración infraestructura de bases de datos.
    - Migración a Windows 10.
    - Migración plataforma de seguridad perimetral (Firewall).
    - Ampliación de cabinas de almacenamiento.
    - Implantación de sistema de detección de intrusos.
    - Regularización con nuevas soluciones y mejoras en el entorno de seguridad McAfee (protección adaptable frente a amenazas), cifrado y prevención de pérdida de datos.
    - Nueva plataforma WIFI.

  - Ejecución del plan de mejora de la seguridad tras el incidente:

    - Implementación de autenticación de dos factores en cuentas de administración.

- Despliegue LAPS (solución de contraseña de administrador local) en equipos

- Infraestructura de red con control de acceso por puerto de conexión, filtrado de puerto entre zonas (redes de área local virtual sectorizadas nuevas creadas).

- Refuerzo del bastionado de servidores y equipos (evolución tecnológica).

- Aplicación de políticas de seguridad más restrictivas (directivas de grupo aplicadas en el nuevo dominio).

- Refuerzo en la seguridad en los vectores de ataque por email.

- Sonda de detección de instrucciones y centro de operaciones de seguridad.

- Servicios de centro de operaciones de seguridad de proveedor externo.

- Continuación con la concienciación y formación de los usuarios, con píldoras informativas con mayor frecuencia y directrices de actuación ante indicios y/o sospechas de cualquier intrusión.

- La Comunidad de Madrid publica como RAT de su Consejería de Sanidad, a la que se adscribe el SERMAS y en la que se incluye el Hospital Universitario de Torrejón, lo siguiente : <https://www.comunidad.madrid/sites/default/files/doc/presidencia/13_04rat_consejeriasanidad.pdf>

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

En primer lugar, se debe señalar que, conforme dispone el art 33.1 del RGPD, el obligado a notificar a la autoridad de control una brecha de seguridad corresponde al responsable del tratamiento, y el encargado del tratamiento informará sin dilación indebida al responsable del tratamiento las violaciones de seguridad de los datos personales de las que tenga conocimiento (art 33.2 RGPD).

En el presente caso, y de la documentación aportada por la entidad investigada y la recabada en las actuaciones de inspección, consta que el responsable de los tratamientos de datos personales llevados a cabo por TS es la Consejería de Salud de la CAM, y el encargado de dichos tratamientos es el TS. Así consta acreditado en el Pliego de Prescripciones Técnicas de la concesión administrativa a favor de TS (concesionario), anexo IX, páginas 12 y 13. También consta en el mismo sentido en el contrato aportado por TS (doc 9) de fecha 10/08/2011, en el que se estipula la condición de encargado del tratamiento a la entidad TS.

En consecuencia, este defecto formal a los efectos de la obligación de notificar la brecha de seguridad deberá ser subsanado a fin de evitar en el futuro este tipo de deficiencias (art 33.1 y 2 del RGPD).

En segundo lugar, es importante advertir que tanto los tratamientos de datos personales, el análisis de riesgos respecto de las libertades y derechos de los afectados como las evaluaciones de impacto cuando procedan, no son procedimientos de análisis estáticos, sino que requieren una revisión continua conforme sobrevienen cambios en los tratamientos, bien técnicos, de tipo estructural, temporal, cualitativos y cuantitativos. También procede la revisión continua de los riesgos contemplados y evaluados como consecuencia de las nuevas tecnologías que aparecen el mercado y que pueden afectar a los tratamientos de datos personales en curso poniendo en peligro los derechos y libertades de los titulares.

Por último, conviene diferenciar con claridad la diferencia entre una incidencia de seguridad de otra que comprometa los datos personales de los interesados. La primera se refiere a aspectos técnicos del sistema de información y la segunda a incidentes que pueden afectar a los derechos y libertades de los interesados. Ambas se afrontan mediante distintas técnicas y metodología de gestión de riesgos que, si bien se complementan en muchos aspectos, se diferencian en la finalidad y el bien protegido.

III

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 los datos personales en las circunstancias arriba indicadas, categorizada como brecha de disponibilidad como consecuencia de la instalación de un malware que había superado los análisis de los antivirus instalados en el sistema de información de TS.

No obstante, también consta que TS a través del servicio de Informática, disponía de medidas técnicas y organizativas razonables y proporcionales al riesgo evaluado para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de los datos personales así como la rápida reacción ante la misma al objeto de notificar 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 el responsable y encargado del tratamiento con el asesoramiento del Delegado de Protección de Datos y con la colaboración de expertos externos en la materia.

No consta que la confidencialidad e integridad de los datos personales obrantes en el sistema de información hayan sido comprometidas

También debe valorase la adopción por TS de medidas técnicas, de gestión y procesales, como es la comprobación de todos los sistemas de información similares y la denuncia de los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado, al objeto de comprobar y, en su caso, mejorar la calidad y seguridad de las aplicaciones de gestión de datos personales a fin de garantizar los derechos y libertades de los interesados. Consta también la realización de una auditoría forense como consecuencia de la brecha se seguridad producida, y cuyos resultados deberán ser monitorizados de forma continua en el tiempo.

La documentación generada de todo el proceso de detección, contención, respuesta y recolección y custodia de evidencias ante una brecha de seguridad de los datos personales es también importante de cara a comunicaciones a partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones y elaborar ejercicios de lecciones aprendidas.

Este informe final elaborado 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.

IV

Por lo tanto, se ha acreditado que la actuación de TS, como entidad encargada del tratamiento ha sido proporcional y razonable 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:

- TORREJON SALUD, S.A. (Hospital Universitario de Torrejón) con NIF A85740595 y domicilio en Calle Mateo Inurria S/N, 28850 Torrejón de Ardoz, Madrid.

- CONSEJERÍA DE SANIDAD DE LA COMUNIDAD DE MADRID, con NIF S7800001E y domicilio en Calle de la Aduana, 29, 28013 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.

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