- **Procedimiento Nº: E/04070/2021**

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: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento CENTRO MÉDICO JACINTO LÓPEZ, S.L. con número de registro de entrada O00007128e2100015205 relativa a ciberataque, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos

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:

CENTRO MÉDICO JACINTO LÓPEZ, S.L. con NIF B36399970 con domicilio en C/ AGUSTÍN ROMERO, Nº 5, BAJO - 36600 VILAGARCÍA DE AROUSA (PONTEVEDRA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Se ha requerido información y documentación al responsable del tratamiento y de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa

Información general de la empresa: según la información obrante en AXESOR, la entidad CENTRO MÉDICO JACINTO LÓPEZ, S.L. es una PYME (pequeña) con unos 17 empleados y un volumen de ventas de unos 900.000 euros.

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

Sobre la cronología de los hechos los representantes del responsable han manifestado que:

"-El virus se activó el domingo día 4 de Abril de 2021 a las 09:50 de la mañana, encriptando todos los archivos del equipo informático. El ataque fue recibido a través

de un correo electrónico SPAM que simulaba tener procedencia del Organismo Oficial SERGAS (Servicio Galego de Saúde), el cual fue abierto en un portátil HP en la vivienda particular de […]. En ese momento tenía abierta una conexión segura en remoto vía VPN con el servidor de la clínica. Este ataque cifró de este modo tanto el disco duro principal del servidor, así como un disco duro externo en el cual se realizan las copias de seguridad y que estaba conectado en ese momento.

-[…la empresa que presta el servicio de informática…] contratada recibe comunicación el lunes 5 de abril a las 08:53h de la mañana por teléfono desde el Centro Médico conforme […] no puede acceder a los sistemas. Acudimos presencial e inmediatamente a las instalaciones del Centro Médico, donde pudimos identificar el virus como MAKOP. Las medidas adoptadas fueron retirar el servidor, sustituir el disco duro del servidor por uno nuevo y restaurar una copia que no había sido afectada por encontrarse en un soporte distinto, con fecha del día 28 de Enero de 2021, restaurando el funcionamiento del mismo a las 13:40h de esa mañana. En cuanto al portátil afectado en un primer momento se ha procedido a borrar todo el contenido por completo y reinstalar de nuevo.

-A lo largo de la tarde del lunes 5 de abril contactamos con un laboratorio de recuperación de datos en Madrid “ONRETRIEVAL”, con el que solemos trabajar habitualmente y nos dieron posibilidad de recuperar la información afectada, para lo que se les facilitaron algunos archivos de muestra que, por su localización, no contendrían datos personales. -El martes 6 a las 10:33h de la mañana se realiza por parte del Administrador del Centro, con la colaboración de su Delegado de Protección de Datos, la notificación en el Registro de la Sede Electrónica de la AEPD de la Brecha de Seguridad. “

Respecto de las causas que hicieron posible la brecha

El motivo principal de la brecha ha sido el error humano al abrir el contenido de un correo electrónico infectado.

Respecto de los datos afectados.

Los representantes del responsable han manifestado que el cálculo aproximado de pacientes que han sido atendidos en el Centro desde el 28 de enero hasta el 3 de abril, último día en activo de la clínica antes de la brecha, es de 300 personas cuyos datos han dejado de estar disponibles. Dado que parte de la información clínica también se ha almacenado en soporte físico y que los pacientes reciben una copia de los informes tras su visita, la mayoría de estos datos han podido ser recuperados a través de estas fuentes.

Tipología de los datos afectados. Datos básicos, números de documentos identificativos, datos de contacto, datos de salud, imagen y/o audio.

Comunicación a los afectados. Los representantes del responsable indican que para realizar esta comunicación se han tenido en cuenta los siguientes parámetros:

- El número aproximado de afectados: 300 personas

- Las características de la brecha, que impiden conocer exactamente la identidad de los afectados.

- Las características del Centro, que se especializa en rehabilitación, por lo que las visitas de los afectados tienden a ser recurrentes.

Por estos motivos, indican que el Centro ha decidido informar a todos sus pacientes mediante carteles informativos e incluso en la breve entrevista en la recepción del Centro que, si han acudido a las instalaciones como pacientes en las fechas comprendidas entre el 28 de enero de 2021 y el 3 de abril de 2021, nos lo hagan saber para poder informarles personalmente de una brecha de seguridad que afecta a la disponibilidad de su información, para poder subsanar sus consecuencias de la mejor medida posible. Aportan copia del citado cartel.

Sobre el acceso o la utilización por terceros de los datos personales afectados por la brecha, y posible publicación en Internet los representantes de la entidad indican que una vez realizadas las tareas de búsqueda en redes, no se ha encontrado ninguna publicación que lo evidencie. no obstante, la dinámica habitual del funcionamiento de este tipo de ramsonware no implica la fuga de información.

Posibles consecuencias: Los representantes de la entidad han manifestado que las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.).

Respecto de las medidas de seguridad implantadas

Los representantes de la entidad han manifestado que:

-Con anterioridad a la brecha se disponía de medidas para proteger la autenticidad de la información, mediante control de acceso de los usuarios con identificadores y contraseñas, que eran actualizadas periódicamente, así como copias de seguridad automatizadas diarias en disco duro externo, y control de acceso a los soportes, encontrándose los mismos en un despacho cuyo acceso está custodiado permanentemente por el personal administrativo del Centro. Estas medidas eran verificadas con una frecuencia aproximada de 3 meses. A nivel normativo, el Centro dispone de Delegado de Protección de Datos, notificado ante la AEPD, es auditado por el mismo anualmente y se está realizando la pertinente Evaluación de Impacto de la actividad de tratamiento que, desgraciadamente, se ha visto afectada por esta brecha.

Aportan copia del contrato de prestación de servicios informáticos suscrito con la empresa prestadora, de fecha 6 de abril de 2021.

-Sobre el motivo por el cual las medidas de seguridad implantadas no han impedido el incidente indican que a pesar de todas las cautelas tomadas, la amenaza enfrentada ha dispuesto del error humano como fuente de entrada. Las salvaguardas aplicadas se han mostrado insuficientes para mitigar la amenaza de manera suficiente por la frecuencia con la que la copia de seguridad se almacenaba en un soporte desconectado.

-Con posterioridad a la brecha se ha puesto a disposición de todo el personal del Centro la infografía del INCIBE para poder identificar un correo electrónico malicioso (https://www.osi.es/sites/default/files/docs/c14-pdf-infografiaidentificar_phishing.pdf), y se han programado actualizaciones formativas para todo el personal. A nivel técnico, las medidas comprenden tanto la conversión del sistema principal de base de datos de modo local a modo online, de modo que será una compañía externa quien, a su vez realice las copias de seguridad deslocalizadas y de modo apropiado. Asimismo, para el resto de información contenida en sistemas informáticos relativa a los pacientes, las copias de seguridad se realizarán de forma distinta.

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 de disponibilidad

La empresa indica que previamente a la brecha, se encontraba realizando la Evaluación de Impacto de la actividad de tratamiento afectada, entre las medidas de seguridad con las que contaba, afirma realizar un control de acceso de los usuarios con identificadores y contraseñas de actualización periódica, para proteger la autenticidad, se realizan también, copias de seguridad diarias en un disco duro externo y en lo que respecta al control de acceso a los soportes, éstos se encuentran en un despacho custodiado permanentemente por el personal administrativo. Asimismo, cuenta con Delegado de Protección de Datos, notificado ante la AEPD. De todo ello se desprende que, con anterioridad a la brecha, la entidad investigada disponía de medidas de seguridad razonables.

La brecha fue posible gracias a un error humano al abrir un correo infectado, que simulaba proceder del SERGAS y que permitió la extensión del virus y el consiguiente cifrado del disco duro principal del servidor, así como de un disco duro externo, en el que se realizaban las copias de seguridad

En cuanto al impacto, se han visto afectados datos básicos, números de documentos identificativos, datos de contacto, datos de salud, imagen y/o audio.

El volumen de Datos se encuentra en el rango de las 300 personas, afirmando que tras la realización de las tareas de búsqueda en redes, no se ha encontrado evidencia alguna de publicación, teniendo en cuenta que lo habitual en este tipo de ramsonware es que no implique fuga de información.

Para evitar que estos hechos se vuelvan a repetir se va a convertir el sistema principal de base de datos pasando, de modo local a modo on line, siendo una compañía externa la encargada de realizar las copias de seguridad. Abordándose también la formación del personal, programando actualizaciones formativas y en el caso concreto que permitió la existencia de la brecha, se ha puesto a disposición del personal, la infografía del INCIBE para poder identificar un correo electrónico malicioso.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD, comunicar a los interesados a través de un cartel en el centro y la rápida adopción de medidas para eliminarla.

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, 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 CENTRO MÉDICO JACINTO LÓPEZ, S.L., con NIF B36399970

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