- **Expediente Nº: E/08082/2021**

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 sufrida por la entidad Outenuve, S.L.U., con CIF B66589995 (en adelante Outenuve) relativa a un ataque informático con ransomware que afecta a la disponibilidad de datos de un número elevado de responsables, se ordena por la Directora 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 en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: primera notificación recibida el 19/02/2021.

Fecha de detección de la brecha: El día 18 de febrero de 2021.

Se han recibido en total 107 entradas correspondientes a notificaciones de brechas relacionadas con el incidente, si bien varias de ellas adicionales o repetidas, que arrojan un total de 98 responsables de tratamientos de datos personales que notifican la brecha, y que tienen en común todas ellas el incidente de seguridad sufrido en Outenuve, que en unas ocasiones actúa como encargado del tratamiento, mientras que en otras actúa como subencargado cuando el encargado del tratamiento directo del responsable es otra entidad, que a su vez ha subcontratado los servicios con Outenuve.

La brecha de seguridad ha consistido en un ***(…)*** de los servicios y plataformas ofertadas por Outenuve, afectando a numerosos datos personales de diversas categorías, la mayoría datos básicos, identificativos y de contacto, de afiliación sindical y en muchas ocasiones datos económicos o financieros y de salud.

Como consecuencia de la brecha, se han abierto investigaciones a Outenuve así como a encargados de tratamiento afectados que subcontrataron con ella. A este respecto, los representantes de Outenuve han indicado, en las actuaciones de investigación, que la brecha ha afectado a varias empresas clientes de Outenuve, entre ellas SOFT TEAM SYSTEMS, SL, con CIF B60960648 (en adelante STS). Al verificarse que entre los productos que oferta esta última se encuentran soluciones integradas de gestión para la Sanidad, con HIS (Sistemas de Información Hospitalarios), con la posibilidad de que ello pueda conllevar un tratamiento de datos de salud de forma masiva, se han iniciado actuaciones de investigación a la misma.

Así, se ha solicitado información y documentación a STS y de la respuesta recibida se desprende lo siguiente:

Los representantes de la entidad manifiestan que la relación de prestación de servicios de Outenuve a STS se centra exclusivamente, en la fecha del incidente sufrido, en el suministro en formato IaaS (Infraestructura como Servicio) de una VM (Servidor Virtual), cuyo objetivo era preparar el servidor para alojar la aplicación de gestión SQL de un futuro nuevo cliente de STS. El acuerdo para el suministro por parte Outenuve de la VM en formato de IaaS se cierra en fecha 15 de diciembre de 2020 con la aceptación del presupuesto cuya copia aportan. En fecha 22 de diciembre de 2020 reciben notificación de Outenuve a través de email de la entrega de la VM como IaaS, cuya copia aportan. El 28 de diciembre de 2020 se procede a la activación de la licencia de las aplicaciones que se utilizarán, cuya copia también aportan.

Los trabajos por parte de STS de preparación de la VM, que implican la configuración, personalización, parametrización y pruebas de funcionamiento de los mismos se inician a partir del 7 de enero de 2021. Una vez finalizada la implantación y preparación de las aplicaciones, se planifica la formación a los futuros usuarios de estas aplicaciones, formación que se realiza los días: 7, 14, 21 y 28 de enero de 2021 y 8 y 15 de febrero de 2021. Hasta la última fecha de formación (15.02.2021) no se han registrado en la VM alojada en Outenuve ninguna información de carácter personal.

En el momento en que se produce el incidente en Outenuve, el 17 de febrero de 2021, origen de la brecha de seguridad que afecta a la VM, no se había aún registrado ninguna información de carácter personal en la VM contratada a Outenuve, por lo que no hubo ningún tipo de afectación ni riesgo para información de carácter personal alguna.

La detección del incidente en STS tiene lugar el día 18 de febrero de 2021 a las 12:00 horas, cuando se intenta acceder a la VM y no es posible hacerlo. En ese momento contactan con Outenuve para reportar que no nos es posible el acceso a la VM, momento en que se nos informa del problema.

A las preguntas formuladas desde la Inspección de Datos de esta Agencia, los representantes de la entidad insisten en que, a fecha del incidente de seguridad, no existen clientes de STS con servicios contratados en Outenuve, que no existe ninguna afectación en los servicios prestados por STS, que no se tratan tampoco datos de salud y que no existen prestaciones de servicios suscritas con clientes de STS que impliquen a Outenuve.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II
Artículos 32, 33 y 34 del RGPD

El artículo 4 apartado 12 del 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."

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.

No obstante, de la documentación aportada por la entidad en el curso de las actuaciones de investigación realizadas se desprende que no ha resultado afectado por la brecha de seguridad sufrida en Outenuve ningún dato personal de los que STS sea responsable o encargado del tratamiento, por cuanto que en el momento del incidente aún no había alojado ninguna información que contuviera datos personales en los servicios o plataformas de Outenuve.

Igualmente, dado lo anterior, no puede exigirse a STS la obligación de notificar la brecha de seguridad a la Agencia Española de Protección de Datos ni a los posibles afectados, tal y como exigen los artículos 33 y 34 del RGPD.

Por último, cabe destacar que no constan ante esta Agencia reclamaciones por parte de posibles clientes de STS afectados.

IV
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción dentro del ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, 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 SOFT TEAM SYSTEMS, SL, con CIF B60960648.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a la parte interesada.

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.

940-200122

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