Expediente Nº: E/06327/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas de oficio por la Agencia Española de Protección de Datos ante la entidad SOCIEDAD INTEGRAL DE VALORACIONES AUTOMATIZADAS, S.A., y teniendo como base los siguientes,

HECHOS

PRIMERO: Con fecha 28/11/2016, tuvo entrada en la Agencia una notificación de quiebra de seguridad realizada por la entidad Sociedad Integral de Valoraciones Automatizadas, S.A. (en lo sucesivo SIVASA), en la que informa sobre un ataque indebido y deliberado a sus sistemas informáticos.

En dicha notificación advierte que los atacantes habrían podido acceder y copiar datos personales de clientes de SIVASA y de Banco Santander, S.A., si bien esta información no permite a los mismos operar en nombre de los afectados.

Para minimizar cualquier riesgo, ha procedido a deshabilitar cualquier acceso on-line a sus sistemas de SIVASA a través de su web o desde los sistemas del citado Banco y viceversa. Añade que realizan un seguimiento activo para detectar cualquier filtración o uso de esos datos.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados. Durante esta fase, y en respuesta al requerimiento que le fue realizado, SIVASA puso de manifiesto los hechos siguientes hechos:

1. SIVASA es una sociedad del Grupo Santander dedicada a la realización de validaciones de tasaciones inmobiliarias.

2. SIVASA tiene contratos para la gestión tecnológica con:

a. INFORMATICA BORSAN, S.L. (BORSAN) para el desarrollo y mantenimiento de la aplicación que gestiona la base de datos y la página web (***WEB.1).
b. PRODUBAN SERVICIOS INFORMATCOS, S.L. (PRODUBAN) que presta el servicio de *Hosting*.

3. SIVASA ha aportado Informe elaborado como consecuencia del ataque informático sufrido por la compañía, en el que figura:

c. El día 15/10/2016, por parte de terceros desconocidos comenzaron a realizar tareas de reconocimiento de los servicios de la página web de SIVASA y el 17 del mismo mes se produjo el ataque ilícito a la misma. PRODUBAN detectó una primera alerta de ataque el 07/11/2016, que fue comunicado a SIVASA,

iniciándose inmediatamente un análisis detallado de la incidencia y su gravedad.

d. El análisis fue finalizado el 18/11/2016, descartándose que el incidente afectara a otras empresas del Grupo Santander u otras sociedades filiales del Grupo Santander. Con fecha 22 de noviembre se denunció a la policía y a la Agencia Española de Protección de Datos.

Se publicó un aviso en la web de Banco de Santander con objeto de difundir a todos los clientes el ataque sufrido y se colaboró para la publicación del incidente en diversos medios de comunicación.

e. Se produjeron cierres temporales de acceso a los Sistemas, con el fin de asegurarse de que en los sistemas no había ningún malware introducido por los atacantes, hasta garantizar la seguridad. Se desconectó la red, para su posterior reapertura una vez revisada la seguridad de los accesos, se revisaron las IP y los permisos de acceso y se reinstalaron los servidores.

f. Se procedió a la monitorización de las cuentas de los clientes y se comunicó por correo postal a los clientes potencialmente afectados por el ataque.

Se obligó a la actualización de las contraseñas a todos los usuarios.

No hay constancia la utilización por terceros de los datos extraídos.

g. El atacante utilizó direcciones IP pertenecientes a un *Hosting* de Holanda y usando una red TOR (red a nivel mundial diseñada para habilitar el anonimato en línea y la evasión de censura).

h. No se ha podido determinar la cantidad de información descargada, no obstante, y por el tráfico saliente, no parece probable que se haya exportado toda la base de datos.

La base de datos tiene información de aproximadamente 500.000 personas físicas con los datos personales de: nombre y apellidos, NIF, domicilio postal, teléfonos de contacto, correo electrónico, número de cuenta de cargo de importe de la tasación, así como datos relacionados con los inmuebles tasados.

Con la información descargada no se puede acceder a los sistemas del Banco de Santander para la realización de transacciones.

SIVASA ha aportado impresión de pantalla del aviso de seguridad publicado en la web www.bancosantander.es

SIVASA ha facilitado copia de una noticia publicada en el medio de comunicación elpais.com.

SIVASA ha aportado escrito de comunicación a los clientes sobre la incidencia.

4. SIVASA aportó el Registro de Incidencias, en el que consta reflejado el ataque sufrido y las acciones realizadas al efecto, así como copia del Documento de Medidas de Seguridad, para acreditar que dispone de todas las medidas de seguridad de los niveles básico y medio, y Auditoria LOPD de octubre de 2015.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

El artículo 9 de la LOPD establece:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

SIVASA tiene como actividad la realización de tasaciones inmobiliarias, que conlleva el tratamiento de los datos personales relativos a las personas que encargan la tasación y los relacionados con los inmuebles asociados, incluida su valoración.

El sistema de información de SIVASA disponía de las medidas de seguridad establecidas en el Reglamento de desarrollo de la LOPD. Esas medidas incluían las de control de acceso, mediante una clave de usuario y contraseña en el caso de ficheros automatizados; y las de gestión de soportes.

En el presente caso, de la información aportada por la propia entidad SIVASA, se acredita que su sistema de información sufrió un ataque indebido y deliberado, el cual permitió acceder y copiar datos personales de clientes de SIVASA relativos a nombre y apellidos, NIF, domicilio postal, teléfonos de contacto, correo electrónico, número de cuenta de cargo de importe de la tasación, así como datos relacionados con los inmuebles tasados.

Según las comprobaciones realizadas, el acceso a los datos registrados en los sistemas de información de SIVASA fue perpetrado en octubre de 2016 por parte de terceros

desconocidos con importantes conocimientos técnicos, utilizando direcciones IP pertenecientes a un *Hosting* de Holanda y usando una red TOR (red a nivel mundial diseñada para habilitar el anonimato en línea y la evasión de censura), por lo que no ha sido posible determinar su autoría.

Esta circunstancia, en sí misma, no es suficiente para exonerar de responsabilidad a SIVASA, siendo necesario para ello que el acceso indebido no se aprovechara de vulnerabilidades del sistema de información atacado que tuvieran causa en una falta de medidas de seguridad adecuadas o en una ineficaz implantación de las mismas. A este respecto, la Sentencia de la Audiencia Nacional de 25/06/2015 ha señalado lo siguiente:

"En interpretación del citado artículo 9, esta Sala ha señalado en múltiples sentencias, (SSAN, Sec. 1ª, de 13 de junio de 2002, Rec. 1517/2001; 7 de febrero de 2003 Rec. 1182/2001; 25-1-2006 Rec. 227/2004; 28 de junio de 2006 Rec. 290/2004 etc), que la obligación que dimana del mismo no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, toda responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica".

En este caso, no se ha constatado que la denunciada haya incumplido la obligación de adoptar de manera efectiva las medidas dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros, por lo que no cabe entender infringido el artículo 9 de la LOPD citado.

Procede tener en consideración la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25 de febrero de 2010 que, en relación con un caso similar al presente, señaló lo siguiente:

"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por el ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www..., descargándose una copia de la misma. Y tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.
El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito del derecho administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1999, de 19 de diciembre (RTC 1991/246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de xxx".

No obstante, aunque en la Sentencia no se considera probada una vulneración del

artículo 9 de la LOPD, sí se apreció una conducta infractora por parte del responsable del fichero, en concreto la vulneración del deber de guardar secreto, considerando la tardanza de la entidad responsable en adoptar un comportamiento activo para impedir que se hicieran públicos en internet los datos personales comprometidos.

En el presente caso, resulta destacable la diligencia observada por parte de SIVASA tras detectarse el acceso indebido a la información para minimizar los riesgos y asegurar sus sistemas (procedido a deshabilitar cualquier acceso on-line y realizó un seguimiento activo para detectar cualquier filtración o uso de esos datos; se produjeron cierres temporales de acceso a los Sistemas, con el fin de asegurarse de que en los sistemas no había ningún malware introducido por los atacantes, se revisaron las IP y los permisos de acceso y se reinstalaron los servidores), habiendo informado, además, a esta Agencia, a la Policía y a los afectados (mediante comunicación postal y avisos en prensa). En consecuencia, de conformidad con la reseñada Sentencia, tampoco procede imputar a la misma una vulneración del artículo 10 de la LOPD.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a SOCIEDAD INTEGRAL DE VALORACIONES AUTOMATIZADAS, S.A.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

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