Procedimiento Nº: A/00393/2014

RESOLUCIÓN: R/00129/2015

En el procedimiento A/00393/2014, instruido por la Agencia Española de Protección de Datos a la entidad DOMO GESTORA DE VIVIENDAS, S.L.U., vista la denuncia presentada por D. ***F.F.F.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 13/01/2017, tuvo entrada en esta Agencia Española de Protección de Datos un escrito de D. ***F.F.F.*** (en lo sucesivo el denunciante) en el que se pone de manifiesto los siguientes hechos:

<<Buscando el CIF en Google, de la comunidad de bienes a la que mi mujer y yo nos apuntamos hace 3 años y que acaba de hacer entrega de las viviendas en las que actualmente vivimos, nos encontramos en Internet con un documento que habíamos entregado hace 2 años a la Gestora que llevó nuestra promoción y que contiene datos sensibles y que no se encuentran protegidos. Domo Gestora S.L, (www.domogestora.com) con CIF… y dirección… es la empresa que gestionó la promoción de… a la que mi mujer y yo nos apuntamos en 2010. Y es en bajo su dominio y espacio de alojamiento donde se encuentran archivos que no deberían estar a la vista de todo el mundo y que deberían ser protegidos por un sistema cifrado SSL>>.

El denunciante describe la forma de acceso a los documentos, y aporta el detalle de la información accedida, en la que figuran los datos personales del denunciante y su esposa. Dicho acceso a la web domogestora.com a través de los resultados de la búsqueda realizada con el buscador Google y el contenido accedido fueron verificados por el inspector actuante.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se tuvo conocimiento de los siguientes extremos, que constan detallados en el Informe de Actuaciones Previas elaborado:

1. Mediante diligencia de fecha 06/02/2014 se realizaron las siguientes comprobaciones:
    a. Realizada una consulta en Google con el parámetro " ***F.F.F.***" restringida al dominio domogestora.com se obtuvo un enlace al documento con URL ***A.A.A.*** consistente en un certificado de aportaciones realizadas en 2010 por Dña. ***D.D.D.*** y el denunciante.
    b. Realizada una consulta en Google con el parámetro " ***D.D.D.***" restringida al dominio domogestora.com, se obtuvieron como respuesta dos enlaces, uno de ellos el citado anteriormente y el segundo correspondiente a la URL ***B.B.B.***, consistente en la relación de aportaciones de Dª ***D.D.D..***
    c. Realizada una consulta en Google con el parámetro " ***E.E.E.***" restringida al dominio domogestora.com se obtuvo un enlace a un documento con URL ***C.C.C.*** consistente en el acta de la Asamblea General Extraordinaria de la sociedad cooperativa constituida para la promoción de las viviendas, de fecha 17/03/2011.

Incorpora un anexo con el nombre y apellidos de los socios asistentes.

d. Se accede al sitio web www.domogestora.com, comprobándose que no existe el fichero robots.txt.

2. De la información y documentación aportada por DOMO GESTORA DE VIVIENDAS, S.L.U. (en lo sucesivo DOMO GESTORA DE VIVIENDAS), entidad responsable de la web domogestora.com, se desprende:

a. Manifiesta la entidad:

<<Respecto al fichero "robots.txt", es de señalar que, una vez recibida la comunicación por parte de la APD y verificado que, efectivamente, se trata de una utilidad o instrumento de seguridad importante que nunca hubiéramos querido obviar, y comprobado que nuestra web no tenía dicho archivo instalado, se procedió inmediatamente a su instalación>>.

Aporta la entidad impresiones de pantalla mediante las que acredita haber creado el mencionado fichero en su web. Acredita igualmente haber solicitado a Google la desindexación de los documentos de su área privada.

b. Aporta la entidad copia del Documento de Seguridad, añadiendo:

<<… se cuenta con los servicios de una empresa de seguridad (Sytek Developer, S.L.) que, entre otros, nos presta los siguientes servicios: trabajos de análisis y corrección de errores, migración de servicios a nuevo servidor dedicado, mantenimiento y soporte técnico anual, auditoría de seguridad (versiones del sistema operativo y software instalados, firewall y seguridad perimetral, puntos de entrada IP, dominio, permisos, usuarios, grupos, registros de sistema y aplicaciones, análisis de logs) y corrección, en su caso, de fallos de seguridad detectados. Se adjunta (anexo V) documento de pruebas de rendimiento.

- Conscientes de la importancia de trabajar en un entorno seguro, nuestra empresa se viene preocupando por mejorar la seguridad de nuestra web y es por ello que se procedió (con anterioridad a la recepción de su solicitud de información) a solicitar a esta misma empresa un proyecto de securización que se adjunta como anexo VI. Dicho proyecto se encuentra en fase de estudio por nuestra parte si bien se tiene prevista su puesta en marcha en breve.

- Así mismo, para evitar ulteriores inconvenientes, hemos procedido a bloquear el acceso a la base de documentación a través de la web. Así mismo, hemos eliminado todo documento con datos sensibles y/o de carácter personal de dicha URL volcando dicha información en una zona restringida de nuestro servidor local sin acceso a través de internet>>.

Examinado el documento de seguridad, se encuentra que está fechado el 13/01/2014 y dispone de unas normas de control de accesos:

<<Tipo de control de acceso:

• Al área privada y de gestión mediante usuario y contraseña para cada usuario…

Características adicionales:

• Dividida en 3 áreas: pública, privada y de gestión. La zona pública no necesita validación; la zona privada está habilitada para clientes que se tienen que validar a través de usuario y contraseña y la zona de gestión está limitada a trabajadores de la empresa que realizan tareas de CRUD (alta, baja, modificación, eliminación) del contenido de la web.

• El directorio donde se aloja la base de datos documental está protegido y no se puede visualizar su contenido.

Requisitos de seguridad:

• Contraseñas de acceso generadas y facilitadas por el personal interno de IT a los usuarios a través de la página de gestión de la aplicación web.

• Requisitos de robustez de las contraseñas: mínimo de 6 caracteres, que contendrá mayúsculas y minúsculas.

• Cambio de contraseñas para la zona de gestión cada: 12 meses>>.

c. Respecto del desarrollo, informa la entidad:

<<El desarrollo de la web domogestora.com fue realizado por un proveedor externo, tanto para su área pública como para el área privada, más sensible al contener datos personales. Aplicamos todos sus criterios y siempre pensamos que se había desarrollado todo lo necesario para la seguridad de nuestros clientes y de sus datos personales. Actualmente no se dispone de un servicio de mantenimiento realizando estas labores el personal interno de nuestra organización. Se anexan los siguientes documentos:
- Anexo VII: Documento "Funcional para Domogestora.com" con las características de la web.
-.Anexo VIII: Documento "especificaciones web para Domogestora" donde nuestra empresa especifica al desarrollador el esquema que requerimos para la web.
- Anexo IX: Correos electrónicos con el proveedor donde se detallan algunos aspectos técnicos del proyecto.
- Anexo X: facturas de dicho proveedor por los trabajos realizados en la web>>.

d. Respecto al consentimiento otorgado por los denunciantes para exponer sus datos a través de Internet, manifiesta la entidad:

<<En lo que respecta al consentimiento de los afectados para exponer los datos en la web, informarles que, bajo nuestro criterio, contábamos con su aceptación tácita y general manifestada a través del acceso y uso continuo de dicha área privada. Así mismo, habían sido informados de esta utilidad durante las Asambleas de comuneros y a título individual cuando solicitaban sus claves de acceso. Por tanto, la empresa ha considerado en todo momento que, con los medios anteriormente descritos, los afectados estaban informados del contenido y finalidades de dicha web. Se adjunta como anexo Xl correo electrónico de aviso de puesta en marcha de la zona privada de la web. Matizar así mismo que el objetivo único de disponer de un área privada es dar un valor añadido a nuestros servicios; algo que, por otro lado, se ha venido valorando positivamente por nuestros clientes>>.

Así, los Servicios de Inspección han estimado que la entidad pretendía habilitar un área privada a través de la que los clientes tuviesen acceso a su información, habiendo fallado las medidas limitativas de control de accesos, lo que posibilitó su acceso por terceros. Además, la falta del fichero robots.txt posibilitó la indexación por buscadores.

e. Añade la entidad:

<<Adicionalmente, consideramos oportuno hacer hincapié en el hecho de que, nada más recibida comunicación por parte de la APD, hemos procedido de manera inmediata a subsanar las circunstancias que permitieron la indexación de dicha documentación. Así mismo, hacer notar que en ningún caso ha sido intención de nuestra entidad causar un perjuicio a nuestros clientes; todo lo contrario, como comentado anteriormente, la puesta en marcha de este servicio ha sido siempre con ánimo de facilitar un valor añadido no obteniendo nuestra empresa, obviamente, ningún tipo beneficio, sino más bien perjuicio, con el hecho en cuestión. Recalcar así mismo, que en Domo Gestora de viviendas, S.L.U. siempre nos hemos preocupado por la seguridad de la información, disponiendo de personal interno IT así como con empresas externas. De hecho, contamos con los servicios de una empresa externa de consultoría que recientemente ha comenzado a asesoramos en materia de LOPD. Adjuntamos como anexo XII contrato de prestación de servicios con dicha empresa>>.

3. Con fecha 24/11/2014, los Servicios de Inspección de la AEPD comprobaron que los documentos relativos al denunciante y su esposa, que eran de acceso público en fecha

06/02/2014, ya no lo eran.

TERCERO: Con fecha 23/12/2014, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), acordó someter a la entidad DOMO GESTORA DE VIVIENDAS a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

Con tal motivo, se concedió a DOMO GESTORA DE VIVIENDAS plazo para formular alegaciones, recibiéndose escrito de fecha 14/01/2015, en el que se muestra conforme con la información contenida en el acuerdo de apertura, señala que no ha tenido intención de causar perjuicio y enumera las mejoras implantadas en sus sistemas de información para subsanar las circunstancias que permitieron la indexación de la documentación objeto de denuncia:

I.- Se ha procedido a activar el archivo robots.txt en la página web www.domogestora.com para evitar la indexación por parte de todos los buscadores de los directorios privados.
II.- Se ha configurado la seguridad en el servidor web (apache) mediante reglas que impiden el acceso al área privada. Concretamente a través de la configuración de archivos htaccess que posibilitan únicamente el acceso a archivos privados desde urls del dominio; urls que sólo son accesibles mediante usuario y contraseña personal encriptada e individual para cada socio.
III.- El servidor web se ha securizado mediante la activación de reglas en el firewall a través de la configuración de IPTABLES y el cierre de puertos que no sean estrictamente necesarios.
IV.- Hemos procedido a contratar un servicio de actualización y mejora integral del área privada de la web www.domogestora.com consistente en el desarrollo de un acceso restringido a través de un esquema seguro basado en nombres de usuario y contraseñas que se almacenarán cifradas y deberán ser cambiadas obligatoriamente por el usuario una vez al año. También se pondrá en marcha un sistema de protección de directorios que contengan archivos sensibles. Estos directorios se alojarán fuera del directorio público; el servidor que los alojará dispondrá de un sistema de seguridad basado en configuración apache htaccess.

Aporta copia del presupuesto aprobado con las especificaciones técnicas correspondientes.

HECHOS PROBADOS

1. La entidad DOMO GESTORA DE VIVIENDAS es titular del sitio web *www.domogestora.com.*

2. Con fecha 13/01/2017, tuvo entrada en esta Agencia Española de Protección de Datos un escrito del denunciante en el que se pone de manifiesto que, utilizando el buscador de Internet Google, a través de la web *www.domogestora.com* resultaban accesibles diversos documentos que el mismo entregó a la entidad DOMO GESTORA DE VIVIENDAS para la adquisición de una vivienda. En la información accedida figuran los datos personales del denunciante y su esposa.

3. Con fecha 06/02/2014, por los Servicios de Inspección de la AEPD se realizaron las siguientes comprobaciones:

a. Realizada una consulta en Google con el parámetro " ***F.F.F.***" restringida al dominio domogestora.com se obtuvo un enlace al documento con URL ***A.A.A.***

consistente en un certificado de aportaciones realizadas en 2010 por Dña. ***D.D.D.*** y el denunciante.

b. Realizada una consulta en Google con el parámetro " ***D.D.D.***" restringida al dominio domogestora.com, se obtuvieron como respuesta dos enlaces, uno de ellos el citado anteriormente y el segundo correspondiente a la URL ***B.B.B.***, consistente en la relación de aportaciones de Dª ***D.D.D..***
c. Realizada una consulta en Google con el parámetro " ***E.E.E.***" restringida al dominio domogestora.com se obtuvo un enlace a un documento con URL ***C.C.C.*** consistente en el acta de la Asamblea General Extraordinaria de la sociedad cooperativa constituida para la promoción de las viviendas, de fecha 17/03/2011. Incorpora un anexo con el nombre y apellidos de los socios asistentes.
d. Se accede al sitio web www.domogestora.com, comprobándose que no existe el fichero robots.txt.

4. La entidad DOMO GESTORA DE VIVIENDAS, en su respuesta al requerimiento de información que le fue efectuado por los Servicios de Inspección de la AEPD, reconoció que su web no disponía de los protocolos *"robots.txt"* y que éstos fueron instalados *"una vez recibida la comunicación por parte de la AEPD".*

5. DOMO GESTORA DE VIVIENDAS solicitó a Google la desindexación de los documentos de su área privada.

6. Con fecha 24/11/2014, los Servicios de Inspección de la AEPD comprobaron que los documentos relativos al denunciante y su esposa reseñados en el Hecho Probado Tercero no eran de acceso público.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

Se imputa a la entidad DOMO GESTORA DE VIVIENDAS el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

El Art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"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 la 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".

El trascrito artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso, –la comunicación o consulta- de datos personales, es un tratamiento sometido a las

exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal contenidos en los ficheros de la entidad DOMO GESTORA DE VIVIENDAS, correspondiendo adoptar las de nivel bajo en atención al tipo de información que contiene, tal como se especifica en el art. 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con accesos a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento define la "autenticación" como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la "identificación" como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

La vulneración de los preceptos citados aparece tipificada como infracción grave en el artículo 44.3.h) de la LOPD, que considera como tal, *"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

En definitiva, la entidad DOMO GESTORA DE VIVIENDAS está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para sus ficheros, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en los mismos. Sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, al haberse constatado la posibilidad de acceder, sin restricción alguna, a los datos personales aportados por las personas inscritas en dicha entidad.

En concreto, consta acreditado que a utilizando el buscador Google resultaron accesibles los datos personales del denunciante y su esposa publicados a través de la web domogestora.com, contenidos en documentos que detallaban las aportaciones realizadas en el marco de una promoción de viviendas en la que aquéllos participaron, así como los datos personales de otros socios de la sociedad cooperativa a la que pertenecían todos ellos.

Asimismo, consta que este acceso pudo llevarse a cabo por una deficiente implantación de las medidas de seguridad que hubiesen evitado la indexación de los documentos en cuestión por buscadores de Internet.

Este acceso a los datos personales reseñados supone la comisión, por parte de DOMO GESTORA DE VIVIENDAS, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que tales hechos se producen por una deficiente implementación de las medidas de seguridad obligatorias según la naturaleza y el nivel de seguridad asignado al fichero en cuestión, según ha reconocido la propia entidad imputada.

Asimismo, las deficiencias de seguridad en los sistemas de información de quedan

igualmente probadas considerando las medidas implementadas como consecuencia del incidente de seguridad reseñado. DOMO GESTORA DE VIVIENDAS, una vez tuvo conocimiento de la denuncia, instaló los protocolos *"robots.txt"* para evitar la indexación por buscadores, solicitó a Google la desindexación de los documentos de su área privada y contrató a una entidad tercera para la implantación de las mejoras detalladas en el Antecedente Tercero.

Así, los datos personales de los socios de DOMO GESTORA DE VIVIENDAS resultaron accesibles a terceros por una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Por tanto, dado que existió una vulneración del *"principio de seguridad de los datos"*, se considera que DOMO GESTORA DE VIVIENDAS ha incurrido en la infracción grave descrita.

III

El artículo 45.6 de la LOPD, introducido a través de la reforma operada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, dispone:

Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento."

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que la infracción de la LOPD de la que se responsabiliza al denunciado es una infracción "grave"; que el denunciado no ha sido sancionado o apercibido por este organismo en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD. Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD **no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.**

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella y cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las

actuaciones.

Como se ha señalado, en el asunto que examinamos la denunciada adoptó con diligencia las medidas correctoras necesarias para adecuar su conducta a las exigencias de la LOPD. En concreto, según consta en el Documento de Seguridad aportado, se ha dispuesto el acceso al área privada mediante usuario y contraseña, el directorio donde se aloja la base de datos documental está protegido y no se puede visualizar su contenido, y las contraseñas de acceso, que se facilitan por el personal interno a través de la página de gestión de la aplicación web, tendrán un mínimo de 6 caracteres, que contendrá mayúsculas y minúsculas.

Por otra parte, ha procedido a activar el archivo robots.txt en la página web www.domogestora.com para evitar la indexación por parte de todos los buscadores de los directorios privados, se configurado la seguridad en el servidor web (apache) mediante reglas que impiden el acceso al área privada, el servidor web se ha securizado mediante la activación de reglas en el firewall a través de la configuración de IPTABLES y el cierre de puertos que no sean estrictamente necesarios y se ha contratado un servicio de actualización y mejora integral del área privada de la web consistente en el desarrollo de un acceso restringido a través de un esquema seguro basado en nombres de usuario y contraseñas que se almacenarán cifradas y deberán ser cambiadas obligatoriamente por el usuario una vez al año. También se pondrá en marcha un sistema de protección de directorios que contengan archivos sensibles.

A la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) referente a los supuestos en los que **la denunciada ha adoptado las medidas correctoras oportunas,** de acuerdo con lo señalado **se debe proceder al archivo de las actuaciones.**

De acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1.- ARCHIVAR el procedimiento **A/00393/2014** seguido contra la entidad DOMO GESTORA DE VIVIENDAS, S.L.U., con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD.

2.- NOTIFICAR el presente Acuerdo a la entidad DOMO GESTORA DE VIVIENDAS, S.L.U. y a D. ***F.F.F.***.

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos