Procedimiento Nº: A/00194/2013

RESOLUCIÓN: R/00136/2014

En el procedimiento A/00194/2013, instruido por la Agencia Española de Protección de Datos a la entidad ANDROMEDA SISTEMAS DE INFORMACION, S.L., vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 25/11/2012, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que pone de manifiesto los siguientes hechos:

El denunciante, cliente de la entidad ANDROMEDA SISTEMAS DE INFORMACIÓN, S.L. (en lo sucesivo ANDROMEDA), procedió a abrir una incidencia (tickets), comprobando posteriormente que, utilizando su identificación de usuario y contraseña, podía acceder a incidencias de otros clientes así como a las respuestas que la entidad emitía en relación con las mismas. Entre los datos que figuran accesibles se encuentran: últimos dígitos de cuentas bancarias, códigos de usuarios y contraseñas, nombre de empresas y de personas físicas, direcciones de correo electrónico y números de teléfonos móviles.

Aporta impresiones de pantalla con el resultado de los accesos realizados por el denunciante a través de la web de "HOSTING LMI", en las que figuran datos de otros usuarios relativos de nombre y apellidos, DNI, números de teléfono, usuario y contraseña.

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. En la web HOSTING LMI (www.hostinglmi....) figura como titular de la misma la empresa ANDROMEDA. En dicha web figura que dicha empresa realiza "*el alojamiento de páginas web's, hosting compartido, alojamiento comercio electrónico, tiendas virtuales, registro de dominios y servidores dedicado managed (manejados) y Housing*".
2. Con fechas 26 de marzo y 15 de abril de 2013, por los Servicios de inspección se remitieron requerimientos de información a la empresa ANDROMEDA, al domicilio que figura en la "Declaración de Protección de Datos y Privacidad" de la web www.hostinglmi....., como sede social de la compañía, siendo devueltas las cartas por el Servicio de Correos con la indicación de "Desconocido".
3. Con fecha 3 de mayo de 2013, se remitió un nuevo requerimiento de información a la dirección que figura en el Registro Mercantil Central como sede de la compañía citada y, con fecha 22 de mayo y 13 de agosto de 2013, se recibieron contestaciones a los mismos.

   Según en la documentación aportada:

   ANDROMEDA tiene suscrito un contrato de prestación de servicios con la compañía CONCATEL SL, de fecha 02/01/2013 (posterior a los hechos

denunciados). En dicho contrato figura que ANDROMEDA adquirió de la mercantil HOSTING LMI SL su marca y fondo de comercio y la titularidad de los programas informáticos para prestar los servicios de Hosting que desarrolla. El objeto del contrato suscrito entre ANDROMEDA y CONCATEL, S.L. consiste en la externalización en esta última del desarrollo del tratamiento de datos y medidas de seguridad a los efectos de dar cumplimiento de la normativa vigente en materia de protección de datos.

El procedimiento para notificar incidencias por parte de los clientes de ANDROMEDA consiste en que el usuario identificado escribe la incidencia (abrir un tickets) a través de la web y posteriormente uno de los técnicos de CONCATEL, S.L. accede a la web con su usuario y contraseña para dar respuesta.

Sobre las circunstancias que han producido la incidencia que permite a un usuario de la web acceder a los tickets de terceros, en los que figuran datos personales, ANDROMEDA manifestó lo siguiente: "*Al contestar un ticket, el programa nos muestra una pantalla diciendo que se ha completado correctamente. Para salir de esta pantalla hay que pulsar la palabra BACK. Justo debajo de esta palabra, se encuentra un botón con un link que sirve para añadir la información del ticket a la KNOWLEDGE BASE. Esta información es visible para cualquier usuario registrado y en ningún momento se ponderó las consecuencias que ha acarreado el hecho de contestar un ticket por parte de un usuario haciendo uso de esta función…".*

ANDROMEDA manifestó que, una vez tuvo conocimiento de la incidencia, a través del requerimiento de información de la Agencia, ésta fue resuelta de inmediato, adoptando las siguientes medidas. "*Borrado de todos estos artículos de la KNOWLEDGE BASE. Eliminación de dicho botón… (Add Response to KNOWLEDGE BASE). El borrado de la base de datos de la KNOWLEDGE BASE y eliminación del acceso por menú a la KNOWLEDGE BASE*".

ANDROMEDA ha señalado que desconoce el número de usuarios afectados, ya que solo disponen de las copias de las impresiones de pantalla remitidas desde la Agencia y según esta documentación se vieron afectados 2 usuarios con los datos de nombre y apellidos, DNI y teléfono.

No obstante, en la documentación aportada por el denunciante figuran también códigos de usuarios y contraseñas.

ANDROMEDA manifestó que no ha recibido ninguna reclamación por esta incidencia de sus usuarios.

El denunciante figura en ANDROMEDA como persona de contacto de la empresa ROJESS, S.L.

TERCERO: Con fecha 06/11/2013, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la LOPD, acordó someter a la entidad ANDROMEDA 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 citada Ley Orgánica, tipificada como grave en el artículo 44.3.h) de la misma norma.

Con tal motivo, se concedió plazo para formular alegaciones a la entidad ANDROMEDA, que presentó escrito en el que refieren *"las medidas adoptadas a raíz del incidente"*:

. Se elimina la opción de poder añadir una respuesta a la Base de Conocimiento, dejando únicamente operativa la opción [Back], que devuelve al usuario interno al menú principal. Se evita

la adición de cualquier artículo nuevo a la Base de Conocimiento.
. Se borraron de forma manual, y uno por uno, todos los artículos que aparecían en la Base de Conocimiento. Se impide que cualquier usuario pueda ver los artículos que han ocasionado la incidencia.
. La tabla (base de datos) que contenía toda la información de la Base de Conocimiento también ha sido eliminada, lo que evita que pueda ser guardado cualquier nuevo artículo que se intente añadir a la Base de Conocimiento.
. Eliminación del acceso a la Base de Conocimiento en el menú de la aplicación. También en el menú del usuario interno.

HECHOS PROBADOS

1. La entidad ANDROMEDA es titular de la web www.hostinglmi.....

2. A través de la web www.hostinglmi....., los clientes de ANDROMEDA registrados como usuarios pueden notificar incidencias a dicha entidad siguiendo el procedimiento habilitado para ello (abrir un tickets), que posteriormente son respondidas por un técnico, el cual también accede a la web con su usuario y contraseña.

3. Con fecha 25/11/2012, el denunciante, cliente de la entidad ANDROMEDA y usuario registrado en la web www.hostinglmi....., procedió a abrir una incidencia (tickets), comprobando posteriormente que, utilizando su identificación de usuario y contraseña, podía acceder a incidencias de otros clientes y a las respuestas emitidas por dicha entidad, en las que figuran datos personales de otros usuarios relativos de nombre, apellidos, DNI, números de teléfono, usuario y contraseña.

4. Sobre las circunstancias que produjeron la incidencia reseñada en el Hecho Probado Tercero, ANDROMEDA manifestó lo siguiente: "*Al contestar un ticket, el programa nos muestra una pantalla diciendo que se ha completado correctamente. Para salir de esta pantalla hay que pulsar la palabra BACK. Justo debajo de esta palabra, se encuentra un botón con un link que sirve para añadir la información del ticket a la KNOWLEDGE BASE. Esta información es visible para cualquier usuario registrado y en ningún momento se ponderó las consecuencias que ha acarreado el hecho de contestar un ticket por parte de un usuario haciendo uso de esta función…".*

5. En respuesta al requerimiento de información que los Servicios de Inspección e la Agencia efectuaron a la entidad ANDROMEDA, ésta manifestó que, una vez tuvo conocimiento de la incidencia a través de dicho requerimiento, adoptó las siguientes medidas. "*Borrado de todos estos artículos de la KNOWLEDGE BASE. Eliminación de dicho botón… (Add Response to KNOWLEDGE BASE). El borrado de la base de datos de la KNOWLEDGE BASE y eliminación del acceso por menú a la KNOWLEDGE BASE*".

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

El Titulo VII sobre *Infracciones y sanciones*, el artículo 43 de la LOPD establece:

"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

III

Se imputa a la entidad ANDROMEDA 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.

Y el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables".* En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *"toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

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 recabados por ANDROMEDA de los usuarios de su web www.hostinglmi....., correspondiendo adoptar las calificadas de nivel básico, 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. El artículo 81.1 del citado Reglamento señala que *"Todos los ficheros o tratamiento de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"*.

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 acceso 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.

En definitiva, la entidad ANDROMEDA está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

En este caso, los hechos expuestos, en relación con la posibilidad de que por parte de terceros se pudiera acceder, a través de Internet, a los datos personales contenidos en la base de datos de ANDROMEDA, sin haber garantizado la seguridad de tales datos de carácter personal, suponen la comisión, por parte de dicha entidad, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que a través del sitio web www.hostinglmi....., cuya titularidad corresponde a la citada entidad, en el apartado habilitado por la misma para que los clientes puedan notificar incidencias (abrir un tickets), se podía acceder a la información asociada a otros usuarios que habían utilizado el mismo procedimiento para notificar incidencias, con el detalle de sus datos personales (nombre, apellidos, DNI, números de teléfono, usuario y contraseña).

Así, los datos personales de clientes de ANDROMEDA, usuarios de la web www.hostinglmi....., resultaron accesibles a otros clientes, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. La propia entidad ANDROMEDA manifestó ante los Servicios de Inspección de la Agencia Española de Protección de Datos que "*Al contestar un ticket, el programa nos muestra una pantalla diciendo que se ha completado correctamente. Para salir de esta pantalla hay que pulsar la palabra BACK. Justo debajo de esta palabra, se encuentra un botón con un link que sirve para añadir la información del ticket a la KNOWLEDGE BASE. Esta información es visible para cualquier usuario registrado y en ningún momento se ponderó las consecuencias que ha acarreado el hecho de contestar un ticket por parte de un usuario haciendo uso de esta función…".*

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

IV

El artículo 44.3.h) de la LOPD, considera infracción grave:

"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".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que ANDROMEDA ha incurrido en la infracción grave descrita.

V

La Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25/02/2010, en relación con un caso en el que se examina un posible fallo de seguridad en los sistemas de información, señala lo siguiente:

"…la recurrente no realizó actividad alguna, pese a que era consciente del riesgo de una posible revelación o publicidad del fichero…".

"… un comportamiento adecuado y activo de la misma pudo impedir o, al menos, minimizar el riesgo real de revelación de los datos personales de los usuarios. Es decir, su comportamiento omisivo (no advirtiendo de la fuga a los usuarios, no presentando denuncia, no cambiando la contraseña etc.) facilitó o, al menos, no obstaculizó la revelación de los datos…".

"La recurrente, como garante de los datos personales de terceros que figuraban en sus ficheros, no tuvo la diligencia exigible sino que propició la revelación como cooperador necesario por omisión. Siendo ello así, la Sala entiende cometida, como también recoge la resolución impugnada, la infracción del artículo 10 de la LOPD, tipificada en el artículo 44.3.g) de la citada norma, es decir la vulneración del deber de guardar secreto…".

Los criterios contenidos en la Sentencia citada se han tenido en cuenta para no imputar a ANDROMEDA una infracción de lo dispuesto en el artículo 10 de la LOPD, por incumplimiento del deber de secreto en relación con los datos personales de los afectados, considerando la actuación desarrollada por la misma con posterioridad al incidente para regularizar la situación y minimizar los riesgos, que consta detallada en el Hechos Probado Quinto.

VI

El apartado 6 del artículo 45 de la LOPD establece lo siguiente:

"*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".

A este respecto, procede considerar lo establecido en el artículo 45.4 y 5 de la LOPD, que establece lo siguiente:

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:
a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una cualificada disminución de la culpabilidad de la entidad denunciada por la concurrencia de varios criterios de los enunciados en el artículo 45.4 de la LOPD, concretamente, el volumen de tratamientos afectados, el grado de intencionalidad apreciado y que no constan beneficios obtenidos como consecuencia de la comisión de la presunta infracción. Asimismo, se considera que ANDROMEDA tenía implantados procedimientos de identificación y autenticación para usuarios registrados en su web, resultando la infracción de un defecto en el diseño.

Asimismo, se tiene en cuenta la diligencia mostrada por ANDROMEDA para regularizar la incidencia. Los Servicios de Inspección comprobaron que por parte de la citada entidad se adoptaron medidas para evitar que los datos personales de las personas registradas a través de su web a los que se refiere la denuncia puedan ser accedidos por otros clientes, por lo que se entiende que ha adoptado las medidas correctoras adecuadas para la seguridad de los datos personales registrados en sus ficheros y no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00194/2013**) a la entidad ANDROMEDA SISTEMAS DE INFORMACION, S.L., 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, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica, respectivamente, y de conformidad con lo establecido en los artículos 36 y 37.a), f) y n) de la LOPD, que atribuye la competencia **al Director de la Agencia Española de Protección de Datos.**

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.

2.- Debido a que la incidencia quedó regularizada, no se insta por parte de la Agencia la adopción de una concreta medida correctora. No obstante, se solicita se comuniquen las que de forma autónoma decida adoptar sin que quepa realizar valoración alguna por parte de esta institución al no existir medidas específicas cuya adopción garantice que en el futuro no se vuelva a producir infracción como la declarada.

3.- NOTIFICAR el presente Acuerdo a ANDROMEDA SISTEMAS DE INFORMACION, S.L.

4.- NOTIFICAR el presente Acuerdo a D. ***A.A.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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

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