Procedimiento Nº PS/00686/2008

RESOLUCIÓN: R/01378/2009

En el procedimiento sancionador PS/00686/2008, instruido por la Agencia Española de Protección de Datos a la entidad **ARSYS INTERNET, S.L.** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 12/6/2007, el Director de la Agencia Española de Protección de Datos solicita el inicio de actuaciones previas, debido al presunto acceso ilícito a datos personales en los sistemas de información de una empresa dedicada a gestionar dominios de Internet. Junto a la orden de apertura, incluye: Noticia publicada en el periódico El País el día 11/6/2007, en cuyos titulares consta literalmente: *Los datos de 120.000 usuarios españoles en manos de 'ciberpiratas'*.

Igualmente aporta copia de un post publicado en el servidor web con URL **http://www.....X...../.....**en cuyos titulares consta literalmente: *Carckers roban datos de 120.000 clientes de una empresa de hosting Española.*

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se realizó visita de Inspección a la entidad ARSYS INTERNET, S.L. (en lo sucesivo ARSYS), teniendo conocimiento de los siguientes hechos:

a) Respecto de información recabada de Internet.

Mediante diligencia de fecha 14/6/2007 se recaba la siguiente información:

Artículo publicado en ElPais.com según el cual un cliente de la empresa ARSYS asegura haber detectado en su página web un código ActiveX que no había puesto.

En el servidor web de Yahoo (**http://www.....Y.....**) aparece un artículo de Europa Press según el cual Arsys detectó en abril un incidente de seguridad, tomó las medidas “oportunas” y lo denunció a la Guardia Civil.

Un código ActiveX colocado en una página web puede ser ejecutado en los ordenadores que tengan acceso a dicha página web, si está diseñado con fines malintencionados podría tomar el control del ordenador para diversos fines como, el robo de datos, su utilización como emisor de spam, o como intermediario para atacar a otros sistemas, entre otras posibilidades.

b) Respecto de la entidad informante ARSYS.

De la información facilitada por ARSYS durante la visita de Inspección realizada en fecha 2/7/2007 se desprende lo siguiente:

La entidad recibió un aviso el día 24 de abril de 2007 por parte de tres clientes de la entidad informando sobre comportamientos anómalos de los sitios Web de los que son titulares que se encuentran alojados en los sistemas de ARSYS.

Tras un primer análisis por parte de los técnicos de seguridad de ARSYS, se comprueba que en las páginas afectadas (algo mas de 4000, según la entidad) se ha instalado una secuencia de código que, mediante una redirección a un tercer sitio Web ubicado fuera de España – Panamá o Rusia, según los casos -, realiza la descarga de un programa con características de “troyano” que queda instalado en los equipos que acceden a los sitios web comprometidos.

Consta en el Registro de Incidencias de la entidad una entrada correspondiente a la incidencia informada, si bien en dicha entrada consta que el número de dominios comprometidos fue 8.000. Se aprecia en la resolución de la incidencia el establecimiento de una técnica de control, denominado “*captchas*”, cuyo fin es evitar la posibilidad de éxito de ataques automatizados. El sistema consiste en la realización de una pregunta al usuario, variable para cada ocasión, y cuya respuesta no pueda ser automatizada, como por ejemplo, el reconocimiento de una imagen o la respuesta a una pregunta sencilla.

Tras la detección de la intrusión, la entidad abre una incidencia de seguridad, procediendo sus servicios técnicos a eliminar el código malicioso insertado y poniéndose en contacto con los clientes afectados, a los que se solicita el cambio de contraseña a la mayor brevedad.

Consultado el servicio jurídico de la entidad, se concluye la necesidad de interponer una denuncia ante la Guardia Civil, para que esta realice las acciones que estime oportunas para la persecución de los ciberdelincuentes.

Aporta la entidad copia de la denuncia presentada, presentada en fecha 24 de mayo de 2007, en la que consta que un representante de la entidad manifiesta que los intrusos han tenido acceso a datos personales consistentes en nombres y apellidos,

NIF y/o DNI, domicilios, datos bancarios, direcciones de correo electrónico y teléfonos de contacto de los clientes de la entidad, cuentas FTP y bases de datos de los propios clientes de la entidad. Manifiesta igualmente que el número de clientes afectados asciende a unos 100.000.

Dado que los análisis realizados por la entidad no permitían concluir la vulnerabilidad utilizada para la realización de la intrusión, ARSYS decidió contar con los servicios de una empresa especializada en seguridad informática, que realizó una revisión de seguridad del área atacada. La empresa de seguridad concluyó que el ataque había tenido tres fases.

- En una primera fase, se realizó un ataque de inyección de SQL, mediante el cual el atacante pudo averiguar las claves de acceso de los usuarios a los servicios FTP. Las claves de dichos servicios, en el momento del ataque, estaban almacenadas en una base de datos, donde las se encontraban almacenadas en claro (sin cifrar). El módulo de autentificación del acceso FTP era un desarrollo interno de ARSYS.

- En una segundad fase, las claves FTP fueron utilizadas para acceder a los directorios donde los clientes tenían ubicadas las páginas iniciales de sus sitios web, donde se introdujo el código malicioso.

- Posteriormente, y como efecto del código generado, los usuarios que accedieron a los sitios web comprometidos pudieron ser infectados por el código malicioso situado en páginas web fuera de España en función de las medidas de seguridad que tuvieran implementadas en sus sistemas.

Tras el análisis de los "*logs"* de los sistemas, los miembros de la empresa de seguridad llegaron a la conclusión de que ARSYS había sido atacada sistemáticamente durante unos tres meses, durante los cuales el atacante estuvo explorando los sistemas hasta encontrar la vulnerabilidad explotada finalmente. Para la realización del ataque, el atacante se dio de alta como clientes de ARSYS.

Aporta la entidad copia de la auditoría de seguridad realizada, denominada "Revisión de seguridad del aplicativo AREA DE CLIENTES". En dicho documento se informa de la existencia de 25 vulnerabilidades graves, que permiten el acceso a información confidencial. Se realiza en el informe una clasificación de las 46 vulnerabilidades halladas. Los tres tipos más importantes son:

- Inyección de SQL ("*SQL Injection*"), encontrándose 20 vulnerabilidades. Este tipo de vulnerabilidades ponen en peligro la información alojada en las bases de datos de la entidad. Por ello es, en lo que a protección de datos se refiere, una de las vulnerabilidades más peligrosas.

- Guiones de sitio cruzado ("*XSS*" o "*Cross Site Scripting*"), encontrándose once vulnerabilidades. Este tipo de vulnerabilidades ponen en peligro los equipos que acceden a servidores web alojados por ARSYS. El peligro

respecto a la protección de datos seria la inserción de un programa espía en los equipos, de forma que los atacantes podría tener acceso a toda la información del equipo, así como averiguar los sitios web a los que tienen acceso los usuarios del equipo, sus identificadores de usuario y contraseñas.

- Comprobaciones débiles ("*Weak checks*"), encontrándose nueve vulnerabilidades. De difícil clasificación, dichas vulnerabilidades podrían dar, potencialmente, acceso a cualquier servicio del sistema, incluido el acceso a ficheros y bases de datos.

-

Es de destacar también la aparición, en el código fuente de las aplicaciones, de nombres de servidores, bases de datos alojadas en ellos, claves de usuario (incluso de administradores), y claves de acceso de esos usuarios.

ARSYS aporta copia de la auditoria bienal exigida por el Reglamento de Medidas de Seguridad.

Ante la noticia aparecida en prensa relativa a los hechos acaecidos, la entidad decide emitir una nota de prensa aclarando lo sucedido, e informando haber tomado las medidas técnicas y organizativas oportunas. Aporta el representante de la entidad copia de la nota de prensa emitida.

A raíz del incidente de seguridad ocurrido, la entidad ha tomado la decisión de cifrar todas las claves de acceso a los servicios FTP de clientes. Dicho cambio está siendo realizado en varias fases:

- En una primera fase, inmediata a la detección del incidente de seguridad, se contactó con los clientes cuyos sitios web habían sido modificados, informándoles de hecho y urgiéndoles al cambio de la clave.

- En una segunda fase se implementó una función que obliga a los usuarios al cambio de la contraseña, bloqueando el acceso hasta que se produzca el cambio.

- Finalmente se ha comunicado a los clientes la modificación de la política de gestión de contraseñas, con nuevos criterios de autenticación y fortaleza de las claves.

Igualmente, se ha procedido a revisar el código de las aplicaciones, corrigiendo las vulnerabilidades detectadas tras la auditoria de seguridad. En el momento de la Inspección está en proceso de implantación un nuevo módulo de acceso de usuarios, realizándose el acceso por medio de FTP seguro.

Tras las medidas correctivas realizadas, los sistemas de ARSYS han seguido detectando y bloqueando nuevos ataques como el que originó el incidente objeto de la

presente inspección. Se ha detectado que la frecuencia de dichos ataques ha ido disminuyendo con el tiempo, no produciéndose en la actualidad.

Aporta la entidad copia de los modelos de correos electrónicos emitidos por la entidad a sus clientes respecto de la necesidad de los cambios y el cambio de la normativa de gestión de contraseñas. Se aprecia en ellos una presión creciente hacia los clientes para el cambio de contraseñas. También se aprecian una serie de mejoras en la política de claves, al establecer una longitud mínima de clave de ocho caracteres y una métrica de complejidad de las claves.

ARSYS dispone del Documento de Seguridad de los Ficheros con Datos de Carácter Personal. Igualmente dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en el estándar ISO 27001 (estándar internacional dedicado a la gestión de la seguridad de los sistemas de información).

La existencia de un SGSI resulta reveladora de que la entidad está intentando alinearse con estándares internacionales.

Aporta la entidad copia del Documento de Seguridad, así como de los siguientes documentos extraídos del SGSI:

- Normativa de Seguridad de Red, fechado el 22/12/2006.
- Clasificación y uso de la información, fechado el 1/7/2006.
- Plan de Continuidad del Negocio, fechado el 5/2/2007.
- Uso del Cifrado, fechado el 1/7/2006.
- Control de accesos, fechado el 11/10/2006.
- Gestión de Crisis, fechado el 1/7/2006.

Se observa la cercanía de las fechas al incidente de seguridad, lo sugiere en el momento de dicho incidente el SGSI no estaba suficientemente implantado o refinado.

Se han podido realizar las siguientes comprobaciones:

Se accede a la tabla de la base de datos que contiene los identificadores de usuarios y contraseñas asociadas a ellos, verificándose que el campo de dicha tabla que almacena la contraseña de acceso presenta la información cifrada.

Se accede a la tabla de la base de datos que contiene la información histórica sobre los identificadores de usuarios y contraseñas asociadas a ellos, seleccionándose los usuarios que hubiese modificado su contraseña en fecha anterior al 1/5/2007, verificándose que el campo de dicha tabla que almacena la contraseña de acceso presenta la información en claro (sin cifrar). Se comprueba que las claves elegidas resultan débiles, ya sea por su escasa longitud (las hay de apenas cuatro caracteres de longitud) como de su escasa variabilidad (claves solo numéricas, solo mayúsculas, solo minúsculas). Todo ello revela que, antes del incidente, existía una deficiente política de gestión de claves.

Se solicita acceso al código del programa que gestiona la modificación de contraseñas y su cifrado, comprobándose que en el mismo se ha incluido una función de cifrado de las contraseñas según el estándar RC4.

Se solicita el acceso al código del programa que filtra la información de entrada al sistema, a efectos de evitar la realización de ataques de inyección de SQL, verificándose la existencia de una función que filtra los caracteres especiales y las palabras clave del lenguaje SQL al objeto de evitar que puedan ser utilizada para atacar al sistema.

TERCERO: Con fecha 20 de enero de 2009, el Director de la Agencia Española de Protección de Datos acordó iniciar, procedimiento sancionador a ARSYS INTERNET, S.L., por presunta infracción de los artículos 9 y 10 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en el artículo 44.3 apartados h) y g) de dicha norma, pudiendo ser sancionadas cada una, con multa de 60.101,21 a 300.506,05 euros, de acuerdo con el artículo 45.2 de dicha Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio, ARSYS mediante escrito de fecha 21/02/09 formuló alegaciones, solicitando la aplicación del artículo 45.4 y 5 de la LOPD, del 4.4 del Real Decreto 1398/1993, y significando que:

a) La documentación relativa a la implementación del SGSI se redactó con anterioridad al día 23 de abril de 2007, fecha en la que se conoce por ARSYS el ataque de los "hackers", tal y como se expondrá en el siguiente apartado.

b) ARSYS terminó la implementación del SGSI el día 5 de octubre de 2007 como se refrenda en el ya mencionado certificado de la compañía LGAI Technological Center S.A. Por lo tanto resulta notorio que ARSYS ya venía implementando todas las medidas de seguridad exigidas por el SGSI mucho antes de la existencia de los ataques de los "hackers". En efecto, hubiera resultado imposible terminar la implantación de este complejo y exigente sistema en la fecha referida si no se hubiese comenzado la implementación a principios del año 2007.

c) Tal y como pudo comprobar la Agencia en su visita realizada en la fase de actuaciones previas, todas estas medidas va se encontraban proyectadas y en fase de implementación mucho antes de haberse llevado a cabo el atague a los sistemas de ARSYS y, por supuesto, antes de conocer el inicio de las actuaciones previas llevadas a cabo por la AEPD. Así lo indica el propio Acta de Inspección al decir que "Igualmente dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el estándar ISO 27001".

d) La implementación del SGSI, cuyo rigor y nivel de exigibilidad en materia de seguridad supera los objetivos "de mínimos" previstos en la normativa sobre protección de datos, pone de manifiesto su innegable voluntad y diligencia en orden a dotar a sus sistemas

informáticos de los más modernos, eficaces y garantistas medios en materia de seguridad informática.

Finalmente, merece destacarse el hecho de que son muy pocas las compañías españolas que han obtenido las certificación que acredita la implantación de la norma ISO 27001. De hecho, según el sitio web "www.....Z....." - vid. Documento número 4 adjunto al presente escrito - únicamente 30 compañías españolas han obtenido hasta la fecha esta certificación y tan sólo tres compañías del sector donde ARSYS presta sus servicios (T-Svstems. Telefónica v la propia ARSYS) han obtenido la misma.

En definitiva, ARSYS, en el momento del ataque del que fue objeto, no solamente cumplía con todas las obligaciones formales, técnicas y organizativas previstas en la legislación en materia de protección de datos, sino que tenía implementadas o en fase de implementación procedimientos y sistemas que incluyen medidas de seguridad más garantistas que las requeridas por la legislación en materia de protección de datos personales.

b) De la celeridad en la subsanación de las vulnerabilidades del sistema informático de ARSYS y de las soluciones adoptadas con carácter inmediato al ataque perpetrado por el "hacker"

Tal y como se constata en el documento denominado "Análisis Incidente FTP" entregado a la Agencia en la fase de actuaciones previa, el ataque al que se vio sometido ARSYS se resume temporalmente en las siguientes fases:

1. "El día 15 de febrero de 2007 el atacante se da de alta como cliente de ARSYS, proporcionando un NIF y número de cuenta bancaria españoles válidos".

2. "El día 16 de febrero de 2007 un atacante accede al área de clientes "

3. "Después de recorrer e interactuar con varias aplicaciones descubre una vulnerabilidad SQL injection en el parámetro de la url de la aplicación servicios .asp"

4. "El día 17 de febrero de 2007 se reciben 2.136 peticiones a la aplicación servicios.asp que, mediante la vulnerabilidad SQL injection y aprovechando la capacidad de paginación de la aplicación listan los campos CDA_L0G1N y CDA_PASSWORD."

Esto es, tal y como indica el Acta de Inspección, "se realizó un ataque de inyección SQL, mediante el cual el atacante pudo averiguar las claves de acceso de los usuarios a los servicios FTF"

5. "A partir del día 1 de marzo de 2007 podemos encontrar numerosas peticiones periódicas, realizadas desde distintos clientes, contra el área de cliente [...]. Las peticiones van encaminadas a obtener una lista de los servicios registrados por el cliente así como los datos de facturación del cliente."

6. "[…] entre los días 13 y 1 de abril de 2007 (antes de terminar el recorrido por el panel de control) se realiza un ensayo contra los servidores FTP para discernir cuales de las contraseñas capturadas son válidas. "

7. "Cuando se produce el ataque entre los días 21 y 22 de abril, el atacante no falla ninguna de las contraseñas que intenta. "

Sobre este particular, señalamos que no resultó posible que las medidas de seguridad implantadas por ARSYS detectaran el ataque llevado a cabo por los "hackers" puesto que el mismo se estaba realizando desde conexiones legítimas mediante el uso de contraseñas válidas de los clientes de ARSYS que tienen derecho a acceder a sus sistemas. Este extremo es de todo punto relevante y explica en cierta medida la no detección inmediata del posible incidente.

8. "Durante del fin de semana del 21 y 22 de abril usuarios no identificados comprometieron la seguridad de unos 8.000 dominios, utilizando FTP para acceder con las credenciales de usuario y modificar las páginas HTML principales de los dominios.

La modificación realizada en las páginas añade un iframe a un sitio web malicioso, con el objetivo de instalar un troyano en la máquina del cliente que visite el dominio compro". (…)>>

<<….e) El día 24 de abril, la compañía Neutralbit comenzaron a trabajar en el análisis de los sistemas de ARSYS con la finalidad de reconstruir el procedimiento utilizado por el atacante para introducirse en los sistemas de ARSYS.

f) El día 26 de abril, tal y como constata el escrito de Acuerdo de Inicio de Procedimiento Sancionador, ARSYS se puso en contacto con sus clientes con la finalidad de manifestarles la necesidad de cambiar sus contraseñas e informándoles de que en caso de que no modificasen la misma bloquearían temporalmente su acceso por FTP hasta que introdujesen una nueva contraseña en su Panel de Control, y ello con la única finalidad de que las nuevas contraseñas no permitan el acceso de intrusos.

g) Después de dos días ininterrumpidos de trabajo analizando distintas posibilidades se localizó el punto a través del cual los atacantes se habían introducido en los sistemas de ARSYS, procediendo ARSYS a reforzar tal punto de acceso en la misma mañana del día 28 de abril.

h) Posteriormente, ARSYS analizó conjuntamente con Neutralbit cualesquiera otras debilidades que en un futuro pudieran ser utilizadas por "hackers" para atacar al sistema de ARSYS. Es relevante destacar que tales actuaciones no comportan asunción alguna en el sentido de que los sistemas de ARSYS fueran débiles o no cumplieran con las medidas de seguridad legalmente exigibles sino que ARSYS consideró conveniente potenciar la seguridad de cualquier grieta que, por el avance de la técnica, pudiera ser utilizada en un futuro para atacar los sistemas de esta compañía. Como resultado de todas sus actuaciones se elaboró, entre otros, el ya meritado documento "Análisis incidente FTP" (…)

■ *Los dominios "infectados" fueron únicamente 8.264, por lo que el número de clientes afectados fue necesariamente inferior, en concreto 6.686 clientes.*

■ *No se tiene constancia fáctica alguna de que los "hackers" accedieran a datos distintos de los de los titulares de los 8.264 dominios que, finalmente, fueron "infectados". De hecho, no tiene sentido alguno que habiendo podido acceder los "hackers" a los datos de otros clientes distintos de los antes mencionados no los hubieran utilizado para "infectar" un mayor número de dominios. Sobre este particular debe tenerse en cuenta que el atacante no accede en masa a la totalidad de los datos de los clientes sino que en su ataque debía solicitar "pantallazos" de diferentes clientes. Es por ello que, probablemente, por falta de tiempo no pudiera acceder a datos personales distintos de los 6.686 clientes antes referidos.*

(…) Por lo tanto, el acceso a datos de carácter personal por parte de los "hackers" se aleja mucho de los 100.000 clientes que apunta el Acuerdo de Inicio de Procedimiento Sancionador, puesto que serian aproximadamente 800 los particulares cuyos datos personales (principalmente claves y correo electrónico') pudieron ser conocidos por los atacantes (…)

Del mismo modo, es necesario matizar lo establecido en el escrito de Acuerdo de Inicio de Procedimiento Sancionador, pues en ningún caso apareció en el código fuente de las aplicaciones los nombres de servidores, bases de datos alojados en ellos, claves de usuario o claves de acceso de esos usuarios. Así, ni en el Acta de Inspección se hizo constar la existencia de dichos datos ni de la documentación aportada a la Agencia se desprende este hecho……>>

<<…En este mismo sentido, con respecto a la implantación de medidas de seguridad que garanticen que no se vuelva a producir un ataque a los sistemas de ARSYS con similares características al ya perpetrado por los "hackers", tal y como comprobó la Agencia en su visita realizada a las instalaciones de ARSYS el día 2 de julio de 2007, actualmente:

- *si "se accede a la tabla de base de datos que contiene los identificadores de usuarios y contraseñas asociadas a ellos" se puede verificar "que el campo de dicha tabla que almacena la contraseña de acceso presenta la información cifrada ",*
- *"se ha incluido una función de cifrado de las contraseñas según el estándar RC4 ", y*
- *en el programa que filtra la información de entrada al sistema existe "una función que filtra las palabras clave del lenguaje SQL, al objeto de evitar que puedan ser utilizadas para atacar al sistema. "*

Todos estos esfuerzos adoptados por ARSYS se encuentran respaldados por el hecho de que no ha existido o al menos no le consta ninguna otra ruptura

de los sistemas de seguridad de dicha compañía desde el ataque del que fue objeto en Abril de 2007…>>

<<….Sin embargo, insistimos que, en el caso que nos ocupa, mi representada ha sido la víctima de un ataque desmedido en las técnicas y medios empleados, que duró tres meses y que fue realizado por profesionales con actuaciones en el ámbito internacional, que no sólo han vulnerado los sistemas de ARSYS sino también de empresas de reconocido prestigio que cuentan con poderosas medidas de seguridad. Así, tal y como constata el informe denominado "Análisis Incidente FTP", emitido por Neutralbit, "en contacto con un ISP que sufrió un ataque muy parecido en 2006, han confirmado que nunca pudieron determinar el origen de la intrusión y lo achacaron a un troyano introducido en su red interna". ……>>

<<…De conformidad con cuanto expuesto anteriormente y como consecuencia de la aplicación del principio de culpabilidad no puede sino concluirse la ausencia de culpa en la actuación de ARSYS en lo que respecta al acceso no autorizado de terceros a los datos personales de sus clientes, debiendo por tanto decaer la responsabilidad imputada a la misma. ARSYS no solo venía observando la normativa antes de la producción del hecho que se imputa infractor, sino que actuó con la máxima diligencia exigible a un responsable del tratamiento, solventando con rapidez e inmediatez todos los eventuales accesos de terceros a datos de sus clientes, los cuales, de producirse no son resultado de una falta de implementación de medidas de seguridad sino de un ataque desmedido, extraordinario en cuanto a su forma y llevado a cabo y por personas altamente cualificadas y expertas en este tipo de actuación, conocido como cyber-delincuencia….>>

<….En línea con lo anterior, esta representación sostiene, cuanto menos, la ***concurrencia de un error invencible en la actuación de mi representada, en tanto la misma, de conformidad con lo establecido por un tercero independiente en las auditorías bienales a los sistemas de seguridad creía obrar sin incurrir en ninguna conducta ilícita,*** *siendo claro que adoptó todas las medidas que, con base en la información suministrada por dicho tercero, debía adoptar. En efecto, ARSYS actúo en todo momento de buena fe y sin tener conciencia alguna de que su proceder fuera contrario a la normativa en materia de protección de datos de carácter personal y de medidas de seguridad, ya que adoptó todas las medidas que le eran exigibles en materia de seguridad de datos personales.*

Por otro lado, ***la actuación de mi representada ha sido presidida en todo momento por la buena fe*** *lo que, cuanto menos, debería servir para, en el caso hipotético de la imposición de una sanción a mi representada, apoyar la determinación de esa sanción como la correspondiente a un infracción leve y, con apoyo en lo que más tarde se expondrá, en su grado mínimo. Así,* ***fue la propia ARSYS la que denuncié ante la Guardia Civil la existencia de los ataques de los "hackers" y el eventual acceso a datos de carácter personales de sus clientes,*** *filtrándose la referida noticia a la prensa, lo que derivó en el inicio de las actuaciones de la AEPD.*

Sobre este particular, merece destacarse que, en aras a proteger y prevenir los eventuales perjuicios no solo a la propia ARSYS sino y sobre todo a sus clientes, esta compañía no dudo ni por un momento en proceder a formular dicha denuncia, y ello, aún cuando tal actuación podía suponer un riesgo de que la noticia trascendiese del ámbito de la propia compañía, tal y como ha acontecido, al aparecer la noticia en diversos medios de comunicación. …>>

QUINTO: Con fecha 6/03/09 se inició el período de práctica de pruebas.

SEXTO: El 29/04/2009, se emite propuesta de resolución por la Instructora del procedimiento en el sentido que por el Director de la Agencia Española de Protección de Datos se sancione a ARSYS con dos multa de 60.101,21 € (sesenta mil ciento un euro con veintiún céntimos) cada una, por las infracciones de los artículos 9 y 10 de la LOPD, tipificadas como graves en el artículo 44.3.h) y 44.3.g) de dicha norma.

SÉPTIMO: Con fecha 21/05/2009, ARSYS presenta escrito reiterándose en las alegaciones anteriormente manifestadas, y comunica:

<<…A mayor abundamiento, y con una decidida voluntad de superar los "mínimos" exigibles en la normativa de referencia, ARSYS dispone de un Sistema de Gestión de la Seguridad de la Información (en adelante. "SGSI"). basado en el estándar internacional ISO 27001, el cual se comenzó a implementar en mayo de 2006 y que supone la implantación de adicionales y muy garantistas medidas de seguridad informática.

En este punto interesa reiterar lo ya esgrimido en el escrito de Alegaciones al Acuerdo de Inicio respecto de que todas las medidas del SGSI va se encontraban proyectadas y en fase de implementación mucho antes de haberse llevado a cabo el ataque a los sistemas de ARSYS y, por supuesto, antes de conocer el inicio de las actuaciones previas llevadas a cabo por la Agencia.

Finalmente, merece volver a destacarse el hecho de que son muy pocas las compañías españolas que las han obtenido la certificación que acredita la implantación de la norma ISO 27001. De hecho, según el sitio web "www.....Z....." únicamente 35 compañías españolas han obtenido hasta la fecha esta certificación (…)

En definitiva, inmediatamente tuvo conocimiento ARSYS de los ataques a los que estaba siendo sometido, y pese a la complejidad técnica de los mismos, averiguó el punto de acceso utilizado por los "hackers" para acceder a sus sistemas y puso todas las medidas necesarias y suficientes para garantizar la privacidad de sus clientes. Por lo tanto ARSYS actuó en todo momento con una máxima diligencia para evitar cualquier riesgo derivado del ilícito ataque a sus sistemas e implemento nuevas soluciones en evitación de futuros ataques a sus sistemas de información.

En efecto, merece destacarse que, debido a la rapidez e inmediatez en las actuaciones llevadas a cabo por ARSYS, i) el número de clientes afectados no se vio incrementado, ***ii)*** *el lapso temporal durante el cual los atacantes pudieron acceder a los datos fue sumamente breve y* ***ii)*** *no consta que los datos a los que pudieron acceder fueran utilizados para cualquier finalidad distinta de la de, en su caso, modificar la configuración de las páginas iniciales de los clientes.*

Con todo, los intereses de los clientes de ARSYS se vieron rápidamente salvaguardados y a día de hoy tal y como se ha probado a esta Agencia, ARSYS no sólo cumple - como venia haciendo previamente a tan reiterado ataque del hacker- con la totalidad de las medidas de seguridad exigidas por la normativa sobre protección de datos de carácter personal a los ficheros que contienen datos de carácter personal sino también que es una de las compañías españolas que cuenta con más estrictas medidas de seguridad en sus sistemas ficheros y tratamientos (…)

Siendo el caso que la Propuesta de Resolución transcribe lo referido en el escrito de Acuerdo de Inicio sobre el número de clientes de ARSYS cuyos datos fueron conocidos por los "hackers", resulta necesario reiterar que, en ningún caso, fueron 120.000 el número de clientes cuyos datos personales fueron accedidos por los atacantes de ARSYS.

En efecto, si bien resulta probado que ARSYS denunció ante la Guardia Civil el ataque del que había sido objeto y puso en conocimiento de este cuerpo que en los sistemas de ARSYS se encuentra contenida la información de más de 100.000 clientes, ello no implica que los "hackers" accediesen a la información de todos ellos. Así, de la información que maneja ARSYS, y sin perjuicio de la obvia incertidumbre que genera el imposible conocimiento exacto de las actuaciones desplegadas por los "hackers", se desprende que:

- *Los dominios "infectados" fueron únicamente 8.264 y el número de clientes afectados fueron 6.686, puesto que muchos de los clientes eran titulares de más de un dominio.*

- *De la información con la que cuenta ARSYS no se desprende que los "hackers" accedieran a datos distintos de los de los titulares de los 8.264 dominios que, finalmente, fueron "infectados". De hecho, no tiene sentido alguno que habiendo podido acceder los "hackers" a los datos de otros clientes distintos de los antes mencionados no los hubieran utilizado para "infectar" un mayor número de dominios. Sobre este particular debe tenerse en cuenta que el atacante no accede en masa a la totalidad de los datos de los clientes sino que en su ataque debía solicitar "pantallazos" de diferentes clientes.*

Del mismo modo, se hace necesario reiterar que en ningún caso apareció en el código fuente de las aplicaciones los nombres de servidores, bases de datos alojados en ellos, claves de usuario o claves de acceso de esos usuarios. Así, ni en el Acta de Inspección se hizo constar la existencia de dichos datos ni de la documentación aportada a la Agencia se desprende esta concreta circunstancia…>>

HECHOS PROBADOS

PRIMERO: Con fecha 12/6/2007, el Director de la Agencia Española de Protección de Datos solicita el inicio de actuaciones previas, debido al presunto acceso ilícito a datos personales en los sistemas de información de una empresa dedicada a gestionar dominios de Internet. Junto a la orden de apertura, incluye: Noticia publicada en el periódico El País el día 11/6/2007, en cuyos titulares consta literalmente: *Los datos de 120.000 usuarios españoles en manos de 'ciberpiratas'*.

Igualmente aporta copia de un post publicado en el servidor web con URL **http://www....X...../.....** en cuyos titulares consta literalmente: *Carckers roban datos de 120.000 clientes de una empresa de hosting Española* (folios 1 a 3).

SEGUNDO: Mediante diligencia de fecha 14/6/2007 se recaba la siguiente información, respecto de la información recabada de Internet (folios 4 a 11):

Artículo publicado en ElPais.com según el cual un cliente de la empresa ARSYS asegura haber detectado en su página web un código ActiveX que no había puesto.

En el servidor web de Yahoo (**http://www.....Y.....**) aparece un artículo de Europa Press según el cual Arsys detectó en abril un incidente de seguridad, tomó las medidas "oportunas" y lo denunció a la Guardia Civil.

Un código ActiveX colocado en una página web puede ser ejecutado en los ordenadores que tengan acceso a dicha página web, si está diseñado con fines malintencionados podría tomar el control del ordenador para diversos fines como, el robo de datos, su utilización como emisor de spam, o como intermediario para atacar a otros sistemas, entre otras posibilidades.

TERCERO: De acuerdo con la información facilitada por ARSYS durante la visita de Inspección realizada en fecha 2/7/2007:

La entidad recibió un aviso el día 24 de abril de 2007 por parte de tres clientes de la entidad informando sobre comportamientos anómalos de los sitios Web de los que son titulares que se encuentran alojados en los sistemas de ARSYS.

Tras un primer análisis por parte de los técnicos de seguridad de ARSYS, se comprueba que en las páginas afectadas (algo mas de 4000, según la entidad) se ha instalado una secuencia de código que, mediante una redirección a un tercer sitio Web ubicado fuera de España – Panamá o Rusia, según los casos -, realiza la descarga de un programa con características de "troyano" que queda instalado en los equipos que acceden a los sitios web comprometidos.

Consta en el Registro de Incidencias de la entidad una entrada correspondiente a la incidencia informada, si bien en dicha entrada consta que el número de dominios comprometidos fue 8.000. Se aprecia en la resolución de la incidencia el establecimiento de una técnica de control, denominado "*captchas*", cuyo fin es evitar la posibilidad de éxito de ataques automatizados. El sistema consiste en la realización de una pregunta al usuario, variable para cada ocasión, y cuya respuesta no pueda ser automatizada, como por ejemplo, el reconocimiento de una imagen o la respuesta a una pregunta sencilla.

Tras la detección de la intrusión, la entidad abre una incidencia de seguridad, procediendo sus servicios técnicos a eliminar el código malicioso insertado y poniéndose en contacto con los clientes afectados, a los que se solicita el cambio de contraseña a la mayor brevedad.

Consultado el servicio jurídico de la entidad, se concluye la necesidad de interponer una denuncia ante la Guardia Civil, para que esta realice las acciones que estime oportunas para la persecución de los ciberdelincuentes.

Aporta la entidad copia de la denuncia presentada, presentada en fecha 24 de mayo de 2007, en la que consta que un representante de la entidad manifiesta que los intrusos han tenido acceso a datos personales consistentes en nombres y apellidos, NIF y/o DNI, domicilios, datos bancarios, direcciones de correo electrónico y teléfonos de contacto de los clientes de la entidad, cuentas FTP y bases de datos de los propios clientes de la entidad. Manifiesta igualmente que el número de clientes afectados asciende a unos 8.000 (folios 32 a 36).

Dado que los análisis realizados por la entidad no permitían concluir la vulnerabilidad utilizada para la realización de la intrusión, ARSYS decidió contar con los servicios de una empresa especializada en seguridad informática, que realizó una revisión de seguridad del área atacada. La empresa de seguridad concluyó que el ataque había tenido tres fases.

- En una primera fase, se realizó un ataque de inyección de SQL, mediante el cual el atacante pudo averiguar las claves de acceso de los usuarios a los servicios FTP. Las claves de dichos servicios, en el momento del ataque, estaban almacenadas en una base de datos, donde las se encontraban almacenadas en claro (sin cifrar). El módulo de autentificación del acceso FTP era un desarrollo interno de ARSYS.

- En una segundad fase, las claves FTP fueron utilizadas para acceder a los directorios donde los clientes tenían ubicadas las páginas iniciales de sus sitios web, donde se introdujo el código malicioso.

- Posteriormente, y como efecto del código generado, los usuarios que accedieron a los sitios web comprometidos pudieron ser infectados por el código malicioso situado en páginas web fuera de España en función de las

medidas de seguridad que tuvieran implementadas en sus sistemas.

Tras el análisis de los "*logs"* de los sistemas, los miembros de la empresa de seguridad llegaron a la conclusión de que ARSYS había sido atacada sistemáticamente durante unos tres meses, durante los cuales el atacante estuvo explorando los sistemas hasta encontrar la vulnerabilidad explotada finalmente. Para la realización del ataque, el atacante se dio de alta como clientes de ARSYS.

Aporta la entidad copia de la auditoría de seguridad realizada, denominada "Revisión de seguridad del aplicativo AREA DE CLIENTES". En dicho documento se informa de la existencia de 25 vulnerabilidades graves, que permiten el acceso a información confidencial. Se realiza en el informe una clasificación de las 46 vulnerabilidades halladas. Los tres tipos más importantes son:

- Inyección de SQL ("*SQL Injection*"), encontrándose 20 vulnerabilidades. Este tipo de vulnerabilidades ponen en peligro la información alojada en las bases de datos de la entidad. Por ello es, en lo que a protección de datos se refiere, una de las vulnerabilidades más peligrosas.

- Guiones de sitio cruzado ("*XSS*" o "*Cross Site Scripting*"), encontrándose once vulnerabilidades. Este tipo de vulnerabilidades ponen en peligro los equipos que acceden a servidores web alojados por ARSYS. El peligro respecto a la protección de datos seria la inserción de un programa espía en los equipos, de forma que los atacantes podría tener acceso a toda la información del equipo, así como averiguar los sitios web a los que tienen acceso los usuarios del equipo, sus identificadores de usuario y contraseñas.

- Comprobaciones débiles ("*Weak checks*"), encontrándose nueve vulnerabilidades. De difícil clasificación, dichas vulnerabilidades podrían dar, potencialmente, acceso a cualquier servicio del sistema, incluido el acceso a ficheros y bases de datos.

Es de destacar también la aparición, en el código fuente de las aplicaciones, de nombres de servidores, bases de datos alojadas en ellos, claves de usuario (incluso de administradores), y claves de acceso de esos usuarios (folios 43 y 49).

ARSYS aporta copia de la auditoria bienal exigida por el Reglamento de Medidas de Seguridad.

Ante la noticia aparecida en prensa relativa a los hechos acaecidos, la entidad decide emitir una nota de prensa aclarando lo sucedido, e informando haber tomado las medidas técnicas y organizativas oportunas. Aporta el representante de la entidad copia de la nota de prensa emitida.

A raíz del incidente de seguridad ocurrido, la entidad ha tomado la decisión de cifrar todas las claves de acceso a los servicios FTP de clientes. Dicho cambio está siendo realizado en varias fases:

- En una primera fase, inmediata a la detección del incidente de seguridad, se contactó con los clientes cuyos sitios web habían sido modificados, informándoles de hecho y urgiéndoles al cambio de la clave.

- En una segunda fase se implementó una función que obliga a los usuarios al cambio de la contraseña, bloqueando el acceso hasta que se produzca el cambio.

- Finalmente se ha comunicado a los clientes la modificación de la política de gestión de contraseñas, con nuevos criterios de autenticación y fortaleza de las claves.

Igualmente, se ha procedido a revisar el código de las aplicaciones, corrigiendo las vulnerabilidades detectadas tras la auditoria de seguridad. En el momento de la Inspección está en proceso de implantación un nuevo módulo de acceso de usuarios, realizándose el acceso por medio de FTP seguro.

Tras las medidas correctivas realizadas, los sistemas de ARSYS han seguido detectando y bloqueando nuevos ataques como el que originó el incidente objeto de la presente inspección. Se ha detectado que la frecuencia de dichos ataques ha ido disminuyendo con el tiempo, no produciéndose en la actualidad.

Aporta la entidad copia de los modelos de correos electrónicos emitidos por la entidad a sus clientes respecto de la necesidad de los cambios y el cambio de la normativa de gestión de contraseñas. Se aprecia en ellos una presión creciente hacia los clientes para el cambio de contraseñas. También se aprecian una serie de mejoras en la política de claves, al establecer una longitud mínima de clave de ocho caracteres y una métrica de complejidad de las claves.

ARSYS dispone del Documento de Seguridad de los Ficheros con Datos de Carácter Personal. Igualmente dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en el estándar ISO 27001 (estándar internacional dedicado a la gestión de la seguridad de los sistemas de información).

La existencia de un SGSI resulta reveladora de que la entidad está intentando alinearse con estándares internacionales.

Aporta la entidad copia del Documento de Seguridad, así como de los siguientes documentos extraídos del SGSI:

- Normativa de Seguridad de Red, fechado el 22/12/2006.
- Clasificación y uso de la información, fechado el 1/7/2006.
- Plan de Continuidad del Negocio, fechado el 5/2/2007.

- Uso del Cifrado, fechado el 1/7/2006.
- Control de accesos, fechado el 11/10/2006.
- Gestión de Crisis, fechado el 1/7/2006.

Se observa la cercanía de las fechas al incidente de seguridad, lo sugiere en el momento de dicho incidente el SGSI no estaba suficientemente implantado o refinado.

Se han podido realizar las siguientes comprobaciones:

Se accede a la tabla de la base de datos que contiene los identificadores de usuarios y contraseñas asociadas a ellos, verificándose que el campo de dicha tabla que almacena la contraseña de acceso presenta la información cifrada.

Se accede a la tabla de la base de datos que contiene la información histórica sobre los identificadores de usuarios y contraseñas asociadas a ellos, seleccionándose los usuarios que hubiese modificado su contraseña en fecha anterior al 1/5/2007, verificándose que el campo de dicha tabla que almacena la contraseña de acceso presenta la información en claro (sin cifrar). Se comprueba que las claves elegidas resultan débiles, ya sea por su escasa longitud (las hay de apenas cuatro caracteres de longitud) como de su escasa variabilidad (claves solo numéricas, solo mayúsculas, solo minúsculas). Todo ello revela que, antes del incidente, existía una deficiente política de gestión de claves.

Se solicita acceso al código del programa que gestiona la modificación de contraseñas y su cifrado, comprobándose que en el mismo se ha incluido una función de cifrado de las contraseñas según el estándar RC4.

Se solicita el acceso al código del programa que filtra la información de entrada al sistema, a efectos de evitar la realización de ataques de inyección de SQL, verificándose la existencia de una función que filtra los caracteres especiales y las palabras clave del lenguaje SQL al objeto de evitar que puedan ser utilizada para atacar al sistema (folios 25 a 289)

CUARTO: En la Diligencia de comparecencia y recepción de denuncia ante la Guardia Civil, la entidad ARSYS comunicó que: *<<…tal y como consta en los informes aportados, tienen constancia que utilizando ilegítimamente las contraseñas y nombres de usuarios sustraídos, el o los atacantes accedieron a las cuentas de FTP de unos 8.000 clientes, a través de las cuales modificó las páginas de inicio de las webs de dichos clientes, configurándolas para que al visitarlas redirigiera a una pagina web ajena a los denunciantes, desde donde se les descargaba un virus (…) el atacante ha tenido acceso a la información de mas de 100.000 clientes, que obraba en la base de de datos del área de clientes…>>* (folios 34 y 35)

QUINTO: De acuerdo con el formulario de incidencias de Protección de datos 2007 de 27/04/07: *<<…Tras analizar la incidencia se determinó que durante el fin de semana del 21*

y 22 de abril usuarios no identificados comprometieron la seguridad de unos 8.000 dominios, utilizando FTP para acceder con las credenciales de usuario y modificar las páginas HTML principales de los dominios. La modificación realizada a las páginas añade un iframe a un sitio web malicioso…>> (folios 30 y 31).

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

La LOPD en sus art. 1 y 2.1) establece:

"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."

"1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado."

III

Entrando en el análisis de las cuestiones de fondo planteadas en el presente procedimiento sancionador, el artículo 9 de la LOPD, dispone:

"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".

El citado 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 aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

Para poder delimitar cuáles son los accesos que la LOPD 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 a los ficheros el art. 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo. Por su parte, la letra c) del mismo artículo 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"conservación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

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 conservación 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 refiere 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.

Partiendo de tales premisas deben analizarse a continuación las previsiones que el Real Decreto 994/1998, de 11 de junio, vigente en el momento de producción de la infracción, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que continuaba en vigor de acuerdo con lo estipulado en la disposición transitoria tercera de la LOPD, previa para garantizar que no se produzcan accesos no autorizados a los ficheros.

El artículo 2.10 del citado Reglamento de Seguridad considera *"soporte"* al *"objeto físico susceptible de ser tratado en su sistema de información sobre el cual se pueden grabar o recuperar datos"*. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprensivo de todos ellos en congruencia con los preceptos de la LOPD ya expuestos, que tratan de evitar accesos no autorizados a los datos cualquiera que sea el procedimiento u operación para llevarlo a cabo.

El artículo 8 de dicho Reglamento de seguridad establece:

"1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

2. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".

Así, ARSYS estaba 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 a los datos contenidos en tales ficheros por parte de terceros. Sin embargo, ha quedado acreditado que incumplió esta obligación.

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".

De acuerdo con la disposición transitoria tercera de la LOPD, *"hasta tanto se lleven a efecto las previsiones de la Disposición Final Primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley*".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que ARSYS ha incurrido en la infracción grave descrita.

V

Asimismo, el presente procedimiento tiene por objeto determinar las responsabilidades que se derivan de la revelación de los datos contenidos en los ficheros de los clientes de ARSYS que permanecieron accesibles para terceros a través de la red Internet.

El artículo 10 de la LOPD dispone: *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento.

Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y, por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un *"instituto de garantía de los derechos de los*

ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

En el caso que nos ocupa, ha quedado acreditado que se podía acceder sin restricción a través de Internet a los ficheros, que contienen datos de carácter personal relativos a los clientes de ARSYS.

Por tanto, queda acreditado que por parte de ARSYS responsable de la custodia de los datos en cuestión, se vulneró el deber de secreto garantizado en el artículo 10 de la LOPD, al haber posibilitado el acceso no restringido a datos personales sin consentimiento de sus titulares.

VI

El artículo 44.3.g) de la LOPD, califica como infracción grave:

"La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo"

De acuerdo con los fundamentos anteriores, entendemos que por parte de ARSYS se ha producido una vulneración del deber de secreto y dado que dichos documentos contienen información, entre otros, según denunció la propio entidad ante la Guardia Civil a: <<*…nombres, apellidos, NIFs y/o DNIs , domicilios, datos bancarios, e-mail y teléfonos de contacto de sus clientes…*>>, procede calificarla como infracción grave (el subrayado es de la AGPD).

VII

No puede ser tenida en cuenta la alegación de falta de culpabilidad por parte de ARSYS, por cuanto si bien, el principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción*

administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."

El Tribunal Supremo (STS 16/04/91 y STS 22/04/91) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia."* (STS 23/01/98).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."*(SAN 29/06/01).

Así tras la incidencia producida, días después y tras analizar la citada incidencia, la entidad ARSYS acordó, tal como obra en el formulario de incidencias de protección de datos de 2007: *<<…Se reforzó la política de contraseña y los mecanismos de autenticación, incorporando Capchas en los módulos de autenticación para evitar ataques automatizados…"*

VIII

Los hechos constatados en el presente procedimiento constituyen una base fáctica para fundamentar la imputación a ARSYS de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones dándose la circunstancia que la comisión de una, implica necesariamente la comisión de la otra.

Esto es, si un fallo de seguridad en ARSYS permite el acceso a datos de sus clientes, *"…datos personales consistentes en nombres y apellidos, NIF y/o DNI, domicilios, datos bancarios, direcciones de correo electrónico y teléfonos de contacto de los clientes de la entidad, cuentas FTP y bases de datos de los propios clientes de la entidad…"* se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto profesional.

Por lo tanto, aplicando el artículo 4.4 del citado Real Decreto 1398/1993, procede subsumir ambas infracciones en una. Dado que, en este caso, ambas infracciones están tipificadas como graves, se considera que procede imputar únicamente la infracción del artículo 9 de la LOPD como infracción originaria que ha implicado la comisión de la otra.

IX

La Agencia Española de Protección de Datos ha resuelto numerosos procedimientos sancionadores por infracciones en las medidas de seguridad al haber permitido diversas entidades, el acceso a través de Internet a la información de los datos personales y bancarios de sus clientes que obra en sus ficheros. Asimismo la Sala de lo Contencioso Administrativo de la Audiencia Nacional han dictado sentencias en los recursos contencioso–administrativos interpuestos por las entidades sancionadoras. Entre ellas, en la Sentencia de la Audiencia Nacional, Sala de lo Contencioso- Administrativo, Sección Primera, núm. Recurso: 290/2004, de fecha 28 de junio de 2006, en el Fundamento de Derecho Cuarto señala: "*Esta misma Sala, resolviendo supuestos anteriores en los que los hechos se tipificaron a tenor de dicho Artículo 9 de la Ley Orgánica 15/1999, de Protección de Datos, ha establecido la siguiente doctrina (sentencias de 13 de junio de 2002, Reo. 1161/2001, y de 7 de febrero de 2003, Reo. 1182/2003, entre otras):*

No basta, entonces, 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. Así, de nada sirve que se aprueben unas Instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales, si luego no se exige a los empleados del banco la observancia de aquellas instrucciones.

Se impone, en consecuencia, 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 y como manifiesta el Abogado del Estado en la contestación, 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 también es responsable de que las mismas se cumplan y se ejecuten con rigor. En definitiva toda responsable de un fichero (o encargada de tratamiento) debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios o cualesquiera otros datos de carácter personal puedan llegar a manos de terceras personas.

En definitiva, y puesto que XXX es una deudora de seguridad en materia de datos, debe por tanto dar una explicación adecuada y razonable de cómo los datos personales de sus clientes se hallaban a disposición y se podían encontrar por el afectado (en el lapso temporal en que aconteció el incidente) al acceder éste a la información telemática de sus - datos bancarios, siendo insuficiente, según se desprende de la doctrina de la Sala que se acaba de exponer, con acreditar que se adoptaron una serie de medidas, pues dicha entidad bancaria también es responsable de que las mismas se cumplan y ejecuten con rigor."

X

El artículo 45.2, 4 y 5 de la LOPD, establece:

"2. Las infracciones graves serán sancionadas con multa de 60.101,21 euros a 300.506,05 euros."

"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidiencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho, 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."

La aplicación con carácter excepcional del citado artículo 45.5 de la LOPD, exige la concurrencia de al menos uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuricidad del hecho. En el presente caso, teniendo en cuenta las medidas de seguridad que tenía implementadas ARSYS y las que estaban en fase de implementación; el tipo de ataque sufrido por la entidad, que requiere profundos conocimientos técnicos, y la rapidez con la que se atajó el mismo, aplicando especial diligencia en la adopción de una amplia serie de medidas correctoras, tal como queda acreditado en el hecho probado tercero, es por ello que cabe considerar una disminución cualificada de culpabilidad y procede imponer la sanción en su cuantía de 6000 €.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **IMPONER** a la entidad **ARSYS INTERNET, S.L.** por una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 6.000 (seis mil euros) € de conformidad con lo establecido en el artículo 45.2 y 5 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a **ARSYS INTERNET, S.L.**

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario,

se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 5 de junio de 2009

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte