Expediente Nº: E/06382/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de denuncia presentada por don ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 15 de octubre de 2013, tuvo entrada en esta Agencia un escrito de don ***A.A.A.*** en el que se reconoce miembro de la ASOCIACIÓN IRC HISPANO y manifiesta haber recibido en su buzón electrónico un listado remitido por otro miembro, en el que figuraban las contraseñas de acceso a www.irc-hispano.es de once usuarios, si bien estas contraseñas no aparecían asociadas a los respectivos identificadores de usuario.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. En su escrito de contestación al requerimiento de la Inspección de Datos, la ASOCIACION IRC HISPANO se presenta como asociación sin ánimo de lucro que desde 1996 ofrece una red de chats donde los usuarios pueden chatear entre sí. Según se expone, los usuarios en general pueden chatear con nick o apodo registrado o si lo prefieren desde el anonimato en la gran multitud de salas que hay abiertas.

2. La Asociación aclara que los hechos denunciados no han afectado a los usuarios de los servicios, sino que se ha limitado al personal propio de la organización que gestiona dichos servicios, en concreto a los *Operadores internos* que colaboran voluntariamente con IRC Hispano para la gestión de los servicios a los usuarios. Según se expone, la asociación cuenta con un grupo de usuarios internos con categoría especial, denominados "*Operadores*" u "*OPER*" que, bajo un régimen de voluntariado, ayudan a la red a gestionar a los usuarios. Para formar parte de este colectivo el usuario debe cumplir los siguientes requisitos:

   - Firmar un acuerdo de confidencialidad (*La Asociación ha aportado a la Agencia el suscrito por el miembro denunciado).*

   - Adherirse a las normas de administración de la comunidad, "*Manual de Opers*"*.*

   - Cada operador nuevo debe superar un periodo de prueba inicial nunca inferior a 10 días, sin perjuicio de disponer de amplios y demostrados conocimientos del funcionamiento de la red.

   La Asociación ha declarado que dentro del Grupo *OPER* hay varios usuarios con privilegios "*DEVEL",* que tienen acceso a la administración de sistemas, entre los cuales se encontraba el miembro denunciado.

3. La Asociación ha detallado a la Agencia el procedimiento de identificación y autenticación de los usuarios del sitio web, en particular en lo que se refiere a la configuración de las contraseñas, que en el caso de los *OPER* tiene requisitos adicionales.

4. Según expone la Asociación, el miembro denunciado remitió un mensaje electrónico

a la comunidad de Operadores de IRC Hispano "*en flagrante violación de sus obligaciones de confidencialidad para con nuestra entidad, y violando las instrucciones expresas de nuestra entidad en materia de seguridad de la información"*. Este miembro, "*en su calidad de administrador de seguridad de los sistemas de información de la entidad, tenía al efecto establecidos privilegios para poder acceder a los ficheros donde se guardan las claves encriptadas, con el fin de poder supervisar y gestionar de forma adecuada la seguridad de los sistemas de información asociados a los servicios ofrecidos a los usuarios de IRC Hispano"*. Según se relata, "*dentro de sus funciones como administrador de seguridad, comprobó la fortaleza de las claves de los OPERS pero, a continuación, y extralimitándose en sus funciones, y saltándose los procedimientos de seguridad establecidos y la confidencialidad debida, publicó dichas claves en un[a] correo electrónico interno y privado destinado a los otros colaboradores (OPERS) con el objetivo de que dichos OPER cumpliesen con sus obligaciones de seguridad y cambiasen sus claves por otra con la fortaleza adecuada y exigida por la normativa de seguridad en vigor de nuestra entidad."*

5. La Asociación ha declarado que, de acuerdo con el compromiso de confidencialidad adquirido y las normas previstas en el *Manual de Opers,* el miembro denunciado *"era perfectamente consciente de que la filtración de datos personales o confidenciales implica una violación de las normas de seguridad de nuestra entidad, violación que acarrea la pérdida del status de operador. […] Por dichos motivos, nuestra entidad inició un proceso de investigación interna, que concluyó con el cese de las funciones del [denunciado] como operador de nuestra entidad, cese que le fue comunicado por burofax".*

6. La Asociación también ha declarado: "*En las siguientes 24 horas al incidente, todas las contraseñas de operadores difundidas de forma no autorizada por el [denunciado] fueron cambiadas, y se procedió a revisar el protocolo de contraseñas para miembros del personal de IRC Hispano (Manual de OPERs) con una nueva versión que automatiza sin intervención humana la comprobación de la fortaleza de las contraseñas. […] Asimismo, tras el cese en funciones [del denunciado], se ha procedido a la reinstalación de toda la plataforma tecnológica, incluyendo software, bases de datos, nuevos servidores físicos y registro de direcciones IP, con el fin de asegurar cualquier posible vulnerabilidad causada por la difusión no autorizada de claves."*

7. La Asociación ha declarado: "*No hemos recibido ninguna queja formal de ninguno de los operadores afectados, según el procedimiento que tenemos establecido para ello. Únicamente hemos tenido discusiones en una lista de correo privada y reflejado los cambios que hemos establecido en el manual de operadores".*

FUNDAMENTOS DE DERECHO

I

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

II

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece:

"*1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, establece las medidas de seguridad que han de reunir los tratamientos de datos de carácter personal. En particular, el artículo 91, sobre el control de acceso, prevé:

"*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."

El artículo 93, por su parte, establece:

"*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."

En el presente caso, si bien no se ha obtenido constancia de un acceso indebido a los datos de carácter personal de los miembros de la Asociación, resulta procedente valorar la diligencia observada por esta para atajar la incidencia denunciada, que pudo comprometer la seguridad de las cuentas de once de sus miembros, no siendo preciso exigir a la Asociación la adopción de medidas correctoras adicionales.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a la ASOCIACIÓN IRC HISPANO y a don ***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.

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.

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