**Procedimiento Nº: A/00129/2013**

**RESOLUCIÓN: R/02094/2013**

En el procedimiento A/00129/2013, instruido por la Agencia Española de Protección de Datos a la entidad RED TRABAJAR, S.L., vista la denuncia presentada por D. ***C.C.C.***, y en virtud de los siguientes,

## ANTECEDENTES

**PRIMERO:** Con fecha 16 de octubre y 13 de noviembre de 2012, tuvieron entrada en el registro de la Agencia Española de Protección de Datos sendos escritos de D. ***C.C.C.*** (en lo sucesivo el denunciante) en los que pone de manifiesto los siguientes hechos:

Manifiesta que al acceder, con su código de usuario y contraseña, a la web http://es.redtrabajar.com ha visualizado datos personales y curriculares de terceros, con posibilidad de realizar modificaciones sobre ellos.
Asimismo, manifiesta que, en dos ocasiones, al solicitar una nueva contraseña, se le remitieron por correo electrónico desde la dirección trabajar@trabajar.com sus datos de acceso, correspondientes a la dirección de mail y una contraseña sin cifrar, con los que, no obstante, no pudo acceder a su cuenta en la web.

Con su denuncia aporta impresión de accesos a la web http://es.redtrabajar.com y copia de dos correos electrónicos remitidos desde la dirección trabajar@trabajar.com.

**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 las impresiones de pantalla aportadas por el denunciante, de fecha 3 de octubre de 2012, figuran dos casos:
   Datos curriculares asociados a una dirección de mail, una contraseña cifrada, sexo, fecha de nacimiento, ubicación y sector profesional y a una URL.
   Datos curriculares asociados a nombre, apellidos, NIF, domicilio postal y teléfonos.
2. Con fecha 6 de febrero de 2013, desde la Inspección de Datos, se ha accedido a la web http://es.trabjar.com utilizando las claves de identificación y autenticación aportadas por el denunciante a esta Agencia, verificando que se permite el acceso a los datos de nombre y apellidos, ubicación y colectivo así como a datos curriculares y al “perfil privado” donde figuran datos de dirección de mail, teléfono, dirección postal, sexo y nacionalidad del denunciante.
3. Con fecha 23 de mayo de 2013, desde la Inspección de Datos, se ha verificado que cuando un usuario solicita una nueva contraseña por olvido debe remitir la dirección de correo electrónico con la que se registró en la web http://es.trabajar.com y el sistema remite un correo a dicha dirección proporcionado una URL para la recuperación de la contraseña. Este enlace permite elegir una nueva contraseña o que sea el propio sistema quien la genere. En ambos casos remite la clave de usuario y la contraseña sin cifrar a la dirección de correo

electrónico registrada en la web para el usuario
Asimismo se ha verificado que el enlace para recuperar la contraseña se encuentra activo un periodo muy corto de tiempo (aproximadamente 3 minutos).

En el Acta de Inspección E/6752/2012-I/1 realizada con fecha 7 de febrero de 2013 consta lo siguiente:

1. RED TRABAJAR, S.L. es una red profesional que conlleva varios portales de empleo y permite que los usuarios del portal contacten con otros usuarios y con empresas que ofertan empleo. RED TRABAJAR, S.L. es responsable del fichero en el que se registran los datos recabados a través de la web www.redtrabajar.com.
2. Para ser usuario del portal, se debe dar de alta en el mismo utilizando el formulario de "Alta de usuario" disponible en la web. En el proceso de alta se definen los datos que pueden ser públicos y los que son privados, de esta manera el usuario mantiene dos perfiles: perfil público y perfil privado.
   Asimismo, en este proceso de alta el usuario define el tipo de acceso que permite a los datos registrados de su perfil público: habilitado, deshabilitado y solo empresas. De esta manera, un perfil público "habilitado" es accesible a todos los usuarios del portal y un perfil público "solo empresas" es únicamente accesible para las empresas clientes del portal que ofertan empleo. Y un perfil "deshabilitado" no permite el acceso a ningún usuario ni a las empresas.
   El tipo de acceso puede ser modificado por el propio usuario en cualquier momento.
   El perfil privado es accesible exclusivamente al propio usuario y para aquellas empresas en las que el usuario se ha inscrito en una de sus ofertas publicadas en la web.
   A este respecto, desde la Inspección de Datos se ha comprobado que en la web www.redtrabjar.com consta un apartado de "Términos y condiciones del servicio Trabajar" que informa textualmente: "*El candidato debe seleccionar el nivel de privacidad de los datos personales facilitados a Red Trabajar: 1. Privacidad Máxima (Deshabilitado): Tendrán acceso al curriculum actualizado únicamente aquellas empresas a cuyas ofertas el usuario se haya inscrito. Así, la empresa a la que haya inscrito alguna vez el candidato podrá visualizar el currículum actualizado. De este modo, una empresa en la que se inscribió voluntariamente el candidato tendrá acceso al currículum actualizado y completo del usuario. 2.- Privacidad Alta (solo empresas): El currículum actualizado será visible para las empresas en la base de datos de Red trabajar, también, para aquellas empresas a cuyas ofertas se hay inscrito voluntariamente el candidato. 3.- Privacidad Pública (Habilitado): Todos los datos del currículum serán visibles para cualquier usuario que acceda a los listados profesionales disponibles en la web. El candidato podrá modificar el nivel de privacidad a través de su menú privado*".
3. Se ha constatado que al acceder a la opción de "Alta de usuario" se solicita la cumplimentación del formulario disponible en la web con los datos personales de: nombre y apellidos, dirección de correo electrónico, contraseña (que elige el propio usuario), sexo, fecha de nacimiento, ubicación y colectivo.
   Una vez cumplimentado los datos anteriores, el portal obliga a cumplimentar los datos curriculares que aparecen en el perfil público.
   Antes de finalizar solicita los datos de perfil privado que corresponden a: teléfono, código postal, población, teléfono de contacto opcional y dirección postal.
   Una vez cumplimentado, el sistema remite un correo electrónico de bienvenida a la dirección de email cumplimentada recordando las condiciones del servicio y proporcionando un enlace para el acceso a las mismas y otro enlace para posibilitar la baja.
   En este formulario figura la siguiente leyenda: "*Te enviaremos emails sobre tus nuevos contactos. También recibirás newsletters, notificaciones y ofertas especiales que pueden ser de tu interés. Lee los términos y condiciones que aceptas y siempre podrás ajustar tus notificaciones desde tu perfil privado y podrás dejar de recibir cualquier email desde el pie de*

*los mensajes*".

4. Se ha verificado que al acceder al portal utilizando código de usuario y contraseña se muestran los datos de perfil público y privado asociados a esta identificación y autenticación. Los datos de perfil privado corresponden a: dirección de email, teléfono, código postal, población, sexo, fecha de nacimiento, nacionalidad, permiso de trabajo y algunos datos profesionales junto con el curiculum en formato pdf's.
5. Se ha comprobado que, utilizando las claves de identificación y autenticación aportadas por el denunciante, como datos para el acceso, se permite el acceso a su perfil público y privado. Asimismo se ha verificado que, con la mencionada identificación y autenticación, se accede a los usuarios " ***D.D.D.*** " y " ***B.B.B.*** ", usuarios del sistema que el denunciante ha aportado en las impresiones de pantalla adjuntas a su denuncia, a las que accedió con sus claves de acceso y contraseña, verificando que únicamente permite visualizar sus perfiles públicos.
6. Asimismo se ha comprobado que utilizando la URL ***A.A.A.*** aportada por el denunciante se accede al perfil público de " ***B.B.B.*** ".
7. Se ha verificado que una vez identificado y autenticado, el portal oferta la opción de baja, comprobando que una vez realizada la baja no se permite el acceso, arrojando el mensaje "*los datos de acceso no son correctos*".
8. En relación con la posible incidencia de seguridad que ha permitido al denunciante el acceso a datos de terceros, RED TRABAJAR, S.L. manifiesta:

   Durante del mes de septiembre de 2012, se produjo una modificación en la configuración del servidor de caché lo que conllevó un aumento en el tiempo de respuesta del portal.

   Posteriormente se detectó, por parte de empleados de la entidad, que utilizando su identificación como usuarios del portal podían acceder al perfil privado de otros usuarios.

   Una vez detectado el problema se procedió a la anotación en el Registro de Incidencias de la entidad y a su resolución, la cual figura como probada y finalizada en fecha 20/12/2012.

   No hay constancia de que ningún usuario se haya dirigido a la entidad poniendo de manifiesto la incidencia, por lo que consideran que se ha producido en un número limitado de casos teniendo en cuenta que el sistema tiene unos 200.000 usuarios rápidamente se hubieran puesto en contacto con la entidad.

**TERCERO:** Con fecha 28/06/2013, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), acordó someter a la entidad RED TRABAJAR, S.L. a trámite de audiencia previa al apercibimiento, por la presunta 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 RED TRABAJAR, S.L., recibiéndose escrito de la misma en el que reitera que los hechos denunciados se debieron a un fallo del servidor "proxy-caché" que afectó únicamente a cuatro inscripciones y fue rápidamente detectado y solventado (duró tres horas).

Añade que, en diciembre de 2012, tres meses después de haber realizado un cambio al cambio de software del servidor proxy-caché para resolver un problema de rendimiento en el servicio, se detectó un problema de configuración que provocó, en una situación determinada, que la información de identificación de sesión pudiera llegar a ser intercambiada durante unos 30 segundos cuando el usuario llegaba a una página de oferta dentro del portal en la que no existía la imagen subida por la empresa que publica la oferta e iniciaba sesión para apuntarse a esa oferta en menos de 30 segundos, después de que el anterior usuario iniciara sesión. El motivo de

la no existencia de esa imagen se debía a una corrupción en el fichero subido por la empresa.

En el análisis de alcance de la incidencia, se detectó que la empresa problemática había creado 2 ofertas de empleo. La primera oferta de "Atención al público" fue creada el 2 de Octubre de 2012 y estuvo activa durante 4 días, con una recepción total de 118 inscripciones. La segunda oferta de "Promotor" fue creada el 20 de Diciembre de 2012 y estuvo activa durante 7 días con una recepción total de 232 inscripciones. Con la segunda oferta creada por la empresa se detectó el problema 3 horas después de su activación (el número de inscripciones afectadas fue de 4).

Como medida preventiva se decidió la eliminación de la función de proxy-caché y el aumento de potencia del servidor web para compensar la falta de caché en los elementos estáticos.

Finalmente, considerando que subsanó la incidencia, que no ha sido sancionada y que la infracción imputada se califica como grave, estima que concurren los requisitos establecidos para la aplicación del artículo 45.6 de la LOPD.

## HECHOS PROBADOS

1. La entidad RED TRABAJAR, S.L. es responsable del sitio web www.redtrabajar.com, que permite a los usuarios del portal contactar con otros usuarios y con empresas que ofertan empleo. Para ser usuario se requiere la cumplimentación del formulario de “Alta de usuario” disponible en la web con los datos personales relativos a nombre y apellidos, dirección de correo electrónico, contraseña (que elige el propio usuario), sexo, fecha de nacimiento, ubicación y colectivo. Asimismo, el portal requiere cumplimentar los datos curriculares que aparecen en el perfil público y los datos de perfil privado, que corresponden a: teléfono, código postal, población, teléfono de contacto opcional y dirección postal.

Una vez cumplimentado, el sistema remite un correo electrónico de bienvenida a la dirección de correo electrónico facilitada recordando las condiciones del servicio y proporcionando un enlace para el acceso a las mismas y otro enlace para posibilitar la baja.

En el proceso de alta se definen los datos que pueden ser públicos y los que son privados, de esta manera el usuario mantiene dos perfiles: perfil público y perfil privado. Asimismo, en este proceso de alta el usuario define el tipo de acceso que permite a los datos registrados de su perfil público: habilitado, deshabilitado y solo empresas. Este nivel de privacidad puede modificarse por el usuario a través de su menú privado.

2. El denunciante registró sus datos personales y curriculares en la web www.redtrabajar.com.

3. Con fecha 03/10/2012, el denunciante accedió a través de la web www.redtrabajar.com a datos curriculares de un tercero usuario de la citada web asociados a una dirección de mail, una contraseña cifrada, sexo, fecha de nacimiento, ubicación y sector profesional; y a datos curriculares de otro usuario asociados a nombre, apellidos, NIF, domicilio postal y teléfonos.

El denunciante ha manifestado que dicho acceso se realizó con su código de usuario y contraseña.

4. Con fecha 06/02/2013, utilizando las claves de identificación y autenticación aportadas por el denunciante a la Agencia Española de Protección de Datos, por la Inspección de Datos se accedió a la web http://es.trabajar.com, verificando que se permite el acceso a los datos del denunciante relativos a nombre y apellidos, ubicación y colectivo, así como a datos curriculares y al "perfil privado", en el que figuran datos de dirección de mail, teléfono, dirección postal, sexo y nacionalidad.

5. Con fecha 07/02/2013, durante la inspección realizada a RED TRABAJAR, S.L., por los Servicios de Inspección de la Agencia Española de Protección de Datos se verificó lo siguiente:

. Al acceder al portal www.redtrabajar.com utilizando código de usuario y contraseña se muestran los datos de perfil público y privado asociados a esta identificación y autenticación.
. Utilizando las claves de identificación y autenticación aportadas por el denunciante se permite el acceso a su perfil público y privado.
. Con la identificación y autenticación del denunciante se accedió a los usuarios " ***D.D.D.***" y " ***B.B.B.***", a los que correspondía la información accedida por el denunciante, verificando que únicamente permite visualizar sus perfiles públicos.
. Mediante la URL ***A.A.A.*** aportada por el denunciante se accedió al perfil público de " ***B.B.B.***".
. En relación con la incidencia de seguridad reseñada en el Hecho Probado Tercero, los representantes de RED TRABAJAR, S.L. manifestaron lo siguiente:

Durante del mes de septiembre de 2012, se produjo una modificación en la configuración del servidor de caché que conllevó un aumento en el tiempo de respuesta del portal.
Posteriormente se detectó, por parte de empleados de la entidad, que utilizando su identificación como usuarios del portal podían acceder al perfil privado de otros usuarios.
Una vez detectado el problema se procedió a la anotación en el Registro de Incidencias de la entidad y a su resolución, la cual figura como probada y finalizada en fecha 20/12/2012.
No hay constancia de que ningún usuario se haya dirigido a la entidad poniendo de manifiesto la incidencia.

6. Con fecha 23/05/2013, por los Servicios de Inspección de la Agencia Española de Protección de Datos se verificó que cuando un usuario solicita una nueva contraseña el sistema remite un correo a dicha dirección proporcionado una URL para la recuperación de la contraseña. Este enlace permite elegir una nueva contraseña o que sea el propio sistema quien la genere. En ambos casos remite la clave de usuario y la contraseña sin cifrar a la dirección de correo electrónico registrada en la web para el usuario. Dicho enlace se encuentra activo un periodo muy corto de tiempo (aproximadamente 3 minutos).

## 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 RED TRABAJAR, S.L. 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.

Asimismo, 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 RED TRABAJAR, S.L., S.L. a través de la web www.redtrabajar.com, relativos a los usuarios que se inscriben en la misma como demandantes de empleo, correspondiendo adoptar las calificadas de nivel básico,

en atención a la naturaleza de la 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.

El artículo 91 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establece:

*"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 RED TRABAJAR, S.L. 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 el acceso por parte del denunciante a datos identificativos y curriculares de dos usuarios del sitio web www.redtrabajar.com, contenidos en la base de datos de la que es responsable RED TRABAJAR, S.L., 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 tales hechos se producen por un error en el sistema de información diseñado por la propia entidad. Ésta ha reconocido que la incidencia se ocasiona después de una modificación del software que llevaron a cabo en septiembre de 2012. Dicho fallo posibilitó que el denunciante, al acceder al mencionado sitio web con su código de usuario y contraseña, como usuario del mismo, pudiera visualizar los datos personales registrados por otros (dos) usuarios a través de la citada web, recogidos en documentos en formato Word con posibilidad de modificarlos.

Por tanto, los datos personales de usuarios del sitio web www.redtrabajar.com resultaron accesibles a terceros sin que los afectados hubiesen sido informados en tal sentido, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que RED TRABAJAR, S.L. ha incurrido en la infracción grave descrita.

Tales hechos quedaron acreditados por la documentación aportada por el denunciante, que incluía el detalle de la información accedida a través de la web citada, y por las constataciones realizadas por los Servicios de Inspección de la Agencia Española de Protección de Datos, que con fecha 06/02/2013 comprobaron la posibilidad de acceder a la información de dos usuarios de la web www.redtrabajar.com con las claves de usuario y contraseña asignadas al denunciante por el mismo sistema de información. Además, dicha incidencia ha sido reconocida por la propia entidad imputada, cuyos representantes manifestaron a los citados Servicios de Inspección que los empleados de la entidad detectaron que utilizando la identificación de usuarios del portal podían acceder al perfil privado de otros usuarios.

**IV**

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".*

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 de abril de 1991 y STS 22 de abril de 1991) 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 de enero de 1998).

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 29de junio de 2001).

**V**

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 RED TRABAJAR, S.L. ha incurrido en la infracción grave descrita.

**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 establecen 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 grado de intencionalidad apreciado, el escaso volumen de datos comprometido y que no constan beneficios obtenidos como consecuencia de la comisión de la presunta infracción. Además, se tiene en cuenta que la incidencia no resulta de una falta de medidas de seguridad, en general, por cuanto la entidad disponía de un sistema de control de accesos y de identificación y autenticación, que falló en las circunstancias expuestas.

Por otra parte, durante la inspección realizada a RED TRABAJAR, S.L. en fecha 07/02/2013, por los Servicios de Inspección de la Agencia Española de Protección de Datos se verificó que utilizando las claves de identificación y autenticación aportadas por el denunciante

únicamente se accedía al perfil público de los dos usuarios a los que correspondía la información que motivó la denuncia, y que ese perfil público, según el sistema configurado por la entidad, puede estar deshabilitado o accesible conforme a las opciones determinadas por el usuario que registra sus datos a través de la web redtrabajar.com, bien posibilitando el acceso a todos los usuarios del portal o sólo a las empresas clientes del mismo. El sistema admite, asimismo, que el usuario modifique en cualquier momento el tipo de acceso.

En relación con el perfil privado de los usuarios, se permite el acceso exclusivamente a aquellas empresas en las que el usuario figure inscrito.

Por tanto, se entiende que RED TRABAJAR, S.L. ha adoptado las medidas correctoras adecuadas y que 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/00129/2013**) a RED TRABAJAR, 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.

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.-** 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, en su caso, adoptar.

**3.- NOTIFICAR** el presente Acuerdo a RED TRABAJAR, S.L.

**4.- NOTIFICAR** el presente Acuerdo a D. ***C.C.C.***.

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