Expediente Nº: E/01124/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el ***AYUNTAMIENTO DE ESTREMERA*** en virtud de denuncia presentada por D.ª ***B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 21 de enero de 2013, tuvo entrada en esta Agencia escrito de D.ª. ***B.B.B.*** (en lo sucesivo la denunciante) en el que denuncia que el Ayuntamiento de Estremera (en lo sucesivo el Ayuntamiento) solicita a sus empleados que les proporcione las contraseñas que utilicen para el acceso a los Sistemas de Información del Organismo.
En la denuncia no se aporta ninguna documentación al respecto.

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:
Tal y como consta en el Acta de Inspección E/1124/2013-I/1 realizada en fecha 8 de octubre de 2013 en el Ayuntamiento de Estremera:

1. El Ayuntamiento de Estremera dispone de siete ordenadores conectados en red a un servidor que se encuentra en el propio Ayuntamiento. Los Sistemas de Información del Ayuntamiento, tanto aplicaciones como ficheros, se almacenan directamente en el servidor.

2. Los empleados del Ayuntamiento acceden a los Sistemas de Información utilizando un sistema de identificación y autenticación basado en código de usuario y contraseña, de tal forma que cada uno de ellos tiene un código de usuario asignado por el Administrador del Sistema según el perfil que corresponde al puesto de trabajo que desempeña.
El procedimiento de asignación de usuarios consiste:

> El Alcalde solicita al Administrador de Sistemas la creación de un usuario.
> El Administrador de Sistemas, en presencia del usuario, crea el código de usuario, con el formato "nombre, apellido" y el propio usuario escribe la contraseña elegida por él, aunque el Ayuntamiento recomienda que mantengan el formato "Aytoxxxx", donde "xxxx" corresponde a cuatro dígitos elegidos por el usuario. El registro de la contraseña no es visible.
> Una vez que el usuario ha registrado su contraseña, el Administrador del Sistema marca las opciones de: "*El usuario no puede cambiar la contraseña*" y "*la contraseña nunca caduca*". Estas opciones se pueden modificar en cualquier momento por el Administrador del Sistema.

A solicitud del usuario se pueden modificar las citadas opciones para que el usuario modifique su contraseña. En caso de olvido de contraseña se anula dicho usuario y se crea uno nuevo.

A este respecto, se ha verificado que donde se almacenan los usuarios de los Sistemas de Información del Ayuntamiento se gestiona a través del sistema operativo WINDOWS SERVER 2003, el cual dispone de una aplicación que permite, entre otras funcionalidades, la gestión de usuarios.

2.1 Se ha verificado que en la fecha de la Inspección hay registrados catorce usuarios, uno de los cuales se encuentra marcado. Lo cual según manifiesta el Ayuntamiento corresponde a un empleado que actualmente no presta servicios en el Ayuntamiento al encontrase en situación de "excedencia" por ese motivo se encuentra deshabilitado.

2.2 Se ha comprobado que en este gestor, únicamente consta el código de usuario y su nombre y apellidos junto con las opciones de: "*El usuario no puede cambiar la contraseña*" y "*la contraseña nunca caduca"*.

2.3 Se ha verificado que al realizar el alta de un usuario el registro de la contraseña no es visible.

3. Respecto de las cuentas de correo electrónico. El Ayuntamiento tiene contratado el servicio de correo electrónico corporativo con la empresa NOMINALIA, en cuyo servidor se alojan tanto las cuentas de correo como el contenido de los buzones.

Cada empleado del Ayuntamiento, así como los Concejales tienen una cuenta de correo propia, con el formato "…….@aytoestremera.es". No hay carpetas compartidas.

El acceso a cada cuenta de correo obliga a la identificación a través de un código de usuario, que ha sido generado por el Administrador del Sistema y una contraseña generada por el propio usuario. Estas contraseñas también se encuentran alojadas en el servidor de NOMINALIA.

El Ayuntamiento tiene contratado con NOMINALIA el dominio aytoextremera.es

El Administrador de Sistema y el Alcalde son las personas autorizadas para dar de alta cuentas de correo y usuarios, utilizando una aplicación que NOMINALIA ha puesto a su disposición.

A este respecto, se ha verificado que:

3.1. En el momento de la Inspección hay registrados once cuentas de usuarios.

3.2. Se ha verificado que para dar de alta una nueva dirección hay que registrar un nombre de cuenta de correo (dirección de correo electrónico) del dominio @aytoextremera.es y registrar una contraseña. El Ayuntamiento manifiesta que es el propio usuario, en presencia del Administrador del Sistema el que introduce la contraseña elegida.

De esta circunstancia no se deduce que el administrador vaya a ser conocedor de la misma, sino únicamente que se encontrará presente físicamente

3.3. Se comprueba que la aplicación permite la modificación de la contraseña.

4. En relación con las manifestaciones de la denunciante donde indica que por parte del Ayuntamiento se ha solicitado a todos los usuarios proporcionen las contraseñas que han elegido para el acceso a los Sistemas de Información, el Ayuntamiento manifiesta que en ningún momento se ha solicitado las contraseñas a los usuarios.

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

La denunciante expone que en el Ayuntamiento el informático está instaurando un sistema por el que exige a sus empleados que les proporcione las contraseñas que utilicen para el acceso a los Sistemas de Información del Organismo.

La LOPD en su artículo 9, recoge:

"*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.*

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"

Y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD en su artículo 93, 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".

III

La LOPD en su artículo 40 reconoce a la AEPD la *"potestad inspectora"* y en su apartado 1, recoge: *"Las autoridades de control podrán inspeccionar..."* El Reglamento 1720/2007 de 21/12, por el que se aprueba el Reglamento de desarrollo de la LOPD en su artículo 122 prevé: *" 1…., se podrán*

realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación...” y el R. D. 1398/1993, de 4/08, del Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora en su artículo 12 dispone lo siguiente: “ *Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas de investigación..”*

De acuerdo con la normativa citada corresponde al Director de la Agencia Española de Protección de Datos -AEPD- determinar si, a la vista de la denuncia formulada y de los elementos aportados en justificación de la misma, concurre causa justificativa que lleve a la realización de actuaciones previas de inspección, de suerte que en el presente caso, se realizaron dichas actuaciones previas *“in situ”* con el resultado expuesto en el Hecho Segundo de la presente resolución.

Pues bien, de las diligencias practicadas en el Ayuntamiento se comprueba que el administrador del sistema proporciona un número de usuario que es el nombre y apellidos del usuario y la contraseña la registra el propio interesado, siguiendo las directrices establecidas recomendándose que se mantenga el formato *“Aytoxxxx”, donde “xxxx”* que corresponde a cuatro dígitos a a elección del usuario, no siendo visible el registro de la contraseña.

Una vez que el usuario ha registrado su contraseña, el Administrador del Sistema marca las opciones de: “*El usuario no puede cambiar la contraseña*” y “*la contraseña nunca caduca*” y éstas se pueden modificar en cualquier momento por él y a solicitud del usuario se pueden modificar las citadas opciones para que el usuario modifique su contraseña. En caso de olvido de contraseña se anula dicho usuario y se crea uno nuevo.

También, se ha verificado que donde se almacenan los usuarios de los Sistemas de Información del Ayuntamiento se gestiona a través del sistema operativo WINDOWS SERVER 2003, el cual dispone de una aplicación que permite, entre otras funcionalidades, la gestión de usuarios.

En conclusión, de la inspección no se acredita que se faciliten las contraseñas y no se exige que se tengan que comunicar al informático.

No obstante, se insta a suprimir las referencias *“el usuario no puede modificar la contraseña”* y *“ la contraseña nunca caduca”* al entrar en contradicción con lo dispuesto en el artículo 93.4 del Reglamento de la LOPD y con la posibilidad declarada de que la opción sea modificada por el administrador por el propio usuario.

Por lo tanto, de acuerdo con lo señalado,
Por el Director de la Agencia Española de Protección de Datos,
SE ACUERDA:
PROCEDER AL ARCHIVO de las presentes actuaciones.
NOTIFICAR la presente Resolución al ***AYUNTAMIENTO DE ESTREMERA*** y a D.ª ***B.B.B..***

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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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