Expediente Nº: E/00947/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el AYUNTAMIENTO DE OVIEDO, en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 11 de enero de 2016, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.*** en el que declara lo siguiente:

> Que el fichero que se utiliza en el Servicio de Extinción de Incendios y Salvamento usa una aplicación que no registra los accesos y si ha sido objeto de modificaciones, conforme establece el artículo 103 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo RDLOPD).
>
> El fichero inscrito por los Bomberos está declarado como de nivel alto.
>
> Que en fecha 20 de mayo de 2015, el Ayuntamiento fue informado por un miembro de la Junta de Personal Funcionario del Ayuntamiento de Oviedo unas deficiencias relativas a un registro de acceso a una aplicación informática, que se ordenara la inmediata corrección de las deficiencias expuestas en su escrito, para asegurar y garantizar el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).
>
> Los hechos y las deficiencias que fueron denunciadas se resumen en la existencia de una aplicación informática del Servicio de Extinción de Incendios y Salvamento (en adelante SEIS), propiedad del Ayuntamiento de Oviedo. Dicha aplicación maneja datos de carácter personal que quedan reflejados en los partes de actuación, y que pueden recoger datos de carácter sensible (como pueden ser datos de salud).
>
> Que dicha aplicación, con independencia del número de personas que deben y tienen acceso a la misma, debería de contar con las autorizaciones que cada usuario tiene permitido y con la actividad realiza por cada usuario, ya que si no se estaría vulnerando la LOPD que en su artículo 103 del RDLOPD.
>
> Que pese a dicho escrito no se ha establecido ninguna medida para paliar las deficiencias denunciadas.

Posteriormente, el denunciante aporta copia de la siguiente documentación:

- Escrito con entrada en el AYUNTAMIENTO el día 20 de mayo de 2015 mediante el cual el denunciante informa al mismo de que:
    - Que el SEIS del Ayuntamiento de Oviedo tiene un programa casero (base de datos) para su organización y funcionamiento, operando al margen del sistema municipal de gestión de Datos (FirmaDoc) y que fue realizada por el

inspector ***B.B.B.***, que es quien a su vez se ocupa de su mantenimiento y modificaciones.

- Que no existe control sobre la cantidad de usuarios ni tampoco existe ningún sistema de autenticación ni firma digital que acredite modificaciones en los datos del programa; tampoco existe (como sería de esperar) un historial de edición/borrado de datos para que así quede constancia de los cambios realizados en los datos digitales del servicio.
- Que a fecha del escrito y que se sepa, tiene acceso al programa de gestión de datos mediante clave:

  1 Responsable-interino.

  1 secretaria, (auxiliar administrativa).

  1 Inspector.

  3 sargentos.

  10 subinspectores

  5 operadoras telefónicas del Área de Seguridad Ciudadana.

  1 agente técnico especialista.
- Que el programa de gestión tiene como funciones, distintos menús posibles para el manejo de los siguientes datos privados, susceptibles de sufrir en la actualidad con el actual funcionamiento, modificaciones fraudulentas parciales o totales indetectables causando graves perjuicios e indefensión a terceros.

  - Partes de personal (asistencias, permisos, horas sindicales, vacaciones etc, etc) actividades, prácticas y revisión de vehículos.

  - Informes oficiales de intervención requeridos en ocasiones por particulares o aseguradoras

  - Cuadrantes de mantenimiento de hidrantes, Incidencias (avenas, paralizaciones, reparaciones) en vehículos y llamadas oficiales.

  - Listados de retenes y refuerzos del personal (control de horas extraordinarias).

- Correo electrónico de fecha 15 de septiembre de 2015, emitido por Centralita Bomberos 080, a Jefatura Policía Local con el asunto “Incidencia Lunes DD/MM/AA” en que se informa que el parte de intervención 964 abierto a las 19:14 y cerrado a las 01:02 fue modificado sin el conocimiento de las operadoras telefónicas.
- Escrito fechado el 22 de septiembre de 2015 en que el denunciante informa al AYUNTAMIENTO de la alteración de datos en la aplicación mencionada en la denuncia.
- Capturas de pantalla de la aplicación en las que se muestra que la aplicación admite campos con texto libre, en los que el usuario puede escribir lo que desee.

  Por ello solicita la corrección de las deficiencias encontradas.

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 fecha 10 de junio de 2011 fueron inscritos en el Registro General de Protección de Datos los ficheros BOMBEROS y RECURSOS HUMANOS con códigos de inscripción ***CÓD.1 y ***CÓD.2 respectivamente. Ambos ficheros tienen declaradas medidas de seguridad de nivel alto, al recoger datos de salud.
2. De la información aportada por el AYUNTAMIENTO se desprende:
    a. El nombre del fichero físico origen de la denuncia es una aplicación con denominación *****.mdb, ubicada en los servidores del AYUNTAMIENTO. Se trata de una base de datos en formato Access utilizada para la gestión del Servicio de Extinción de Incendios y Salvamento (SEIS) y que dispone de las siguientes funcionalidades:

- Generación de los siguientes partes (informes*) de:
    - Personal de cada jornada de trabajo.
    - Actividades realizadas en cada jornada de trabajo, donde se asignan las funciones de cada trabajador ese día concreto.
    - Realización de actividades físicas (gimnasia).
    - Realización de prácticas diarias.
    - Mantenimiento de vehículos
    - Intervenciones en emergencias.
    - Jefatura, sobre asuntos varios.
    - Mantenimiento de los desfibriladores semiautomáticos.
    - Incidencias que se observan en los vehículos, herramientas, etc.
    - Llamadas que se realizan desde el Parque de Bomberos y que precisan detallar su contenido.
    - Resúmenes a la Prensa de las intervenciones reseñables.
    - Jornadas de trabajo realizadas por cada persona.
- Generación de faxes a enviar a destinatarios diariamente.
- Gestión de horas extraordinarias que realiza cada trabajador por refuerzos, por retenes especiales o por prolongaciones de jornada.
- Gestión de teléfonos de interés de servicios u organismos relacionados con las emergencias.
- Gestión de calendarios de trabajo de los diferentes turnos de trabajo.
- Envío y recepción de avisos entre los usuarios autorizados con acceso a la aplicación.
- Gestión de relación numérica de las llamadas que entran y salen de la Centralita.
- Control de llaves de las diferentes dependencias del SEIS.

- Información sobre el callejero del municipio.
- Búsqueda selectiva de intervenciones en emergencias, por calle o por número de intervención.
- Gestión de los trabajadores que están ausentes.
- Enlaces a diferentes páginas de Internet con información relacionada con las actividades propias del Servicio de Bomberos.

b. La aplicación trata datos de carácter personal incluidos en los ficheros RECURSOS HUMANOS y BOMBEROS, inscritos en el Registro General de Protección de Datos (RGPD) bajo la titularidad del AYUNTAMIENTO.

c. El AYUNTAMIENTO aporta copia de la estructura de la base de datos, incluyendo todas las tablas que la constituyen y la descripción de los campos de cada una de ellas. Examinado el diseño de las tablas, se observa que muchas de ellas no están destinadas a contener datos de carácter personal, en tanto que las demás están, en general, destinadas aparentemente a contener datos de carácter básico.

d. Aporta igualmente copia de todas las pantallas de que dispone la aplicación. La aplicación cuenta con una pantalla de bienvenida en que se informa al usuario que las condiciones de uso del mismo. Tiene otra pantalla destinada a la Política de Privacidad en donde se informa que la aplicación está destinada a contener datos de carácter básico, por lo que no deben introducirse datos especialmente protegidos.

Examinadas el resto de pantalla aportadas, se encuentra que muchas pantallas no recogen datos de carácter personal, y en las que sí que lo hacen, no se encuentra ninguna en que se soliciten datos que no sean de carácter básico.

e. La identificación y autenticación de los usuarios autorizados para acceder a la aplicación se realiza a través de los mecanismos habilitados en el directorio activo del sistema en el que se ubica la aplicación, mediante la utilización de credenciales personales asignadas a cada usuario (nombre de usuario y clave).

La aplicación dispone de distintos roles en función del tipo de usuario, estando limitado el acceso a ciertos apartados (por ejemplo: apartado administración), mediante clave de acceso asignada a aquellos usuarios autorizados.

Los tipos de usuario que acceden a la aplicación son:

- Los mandos
- Los telefonistas
- Un administrativo
- El responsable de mantenimiento y logística

f. Respecto del registro de accesos, informa el AYUNTAMIENTO que la aplicación está diseñada para cumplir con las medidas de seguridad de nivel básico por lo que dicho registro de accesos no ha sido

establecido.

g. Con el fin de dotar a la aplicación de medidas de seguridad adicionales, se han habilitado las directivas de auditoria de Microsoft Windows Server.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora 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.

II

Los hechos y las deficiencias que fueron denunciadas se resumen en la existencia de una aplicación informática del SEIS, a través de la cual se manejan datos de carácter personal que quedan reflejados en los partes de actuación, y que pueden recoger datos de carácter sensible (como pueden ser datos de salud).

Añaden que dicha aplicación, con independencia del número de personas que deben y tienen acceso a la misma, debería de contar con las autorizaciones que cada usuario tiene permitido y con la actividad realiza por cada usuario, ya que si no se estaría vulnerando la LOPD que en su artículo 103 del RDLOPD.

El artículo 9 de la LOPD 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 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 transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

Sintetizando las previsiones legales citadas 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, regulado en normas reglamentarias.

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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el *"Soporte"* como el "*objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Por su parte el artículo 81.1 del mismo Reglamento señala que "*Todos los ficheros o tratamientos 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. El artículo 88, en su punto 3, se refiere al documento de seguridad.

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.

En el caso presente, se denuncia que la aplicación indicada incumple lo establecido en el artículo 103 del RDLOPD, que sería aplicable en el caso de aplicarse las medidas de seguridad de nivel alto.

"Registro de accesos

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

Tras la realización de las actuaciones previas de investigación, no se ha acreditado que en dicha aplicación se traten datos especialmente protegidos. El Ayuntamiento de Oviedo ha acompañado imágenes con las pantallas de la aplicación en las que se indica que solo se incluirán datos básicos, indicándose que no se deben incluir datos sensibles. En consecuencia, no sería necesario incorporar las medidas de seguridad de nivel alto en la aplicación denunciada.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución al AYUNTAMIENTO DE OVIEDO 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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos