Procedimiento Nº: E/06319/2019
940-0419

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por el Ayuntamiento de Madrid en el que informan a la Agencia Española de Protección de Datos que, con fecha 16 de marzo de 2019, un ciudadano les ha comunicado un incidente de seguridad que permitía el acceso a datos de terceros. La causa que provocó el incidente fue debido a que una dirección (URL) de acceso al trámite del registro electrónico del Ayuntamiento era visible y en ella se incluía el número de registro de la solicitud, de tal forma que modificando dicho número se podía acceder a los datos de solicitud de otro ciudadano.

Con fecha 12 de julio de 2019 se recibe un escrito de ampliación de la notificación, en la que se adjunta un Informe elaborado por Informática del Ayuntamiento de Madrid (IAM) sobre una *Vulnerabilidad de la Sede Electrónica del Ayuntamiento de Madrid* en el que se pone de manifiesto que el Ayuntamiento remitió a IAM, el 20 de marzo de 2019, una comunicación sobre el incidente informado por el ciudadano y una vez estudiado el caso, el equipo de Seguridad de IAM confirmó la veracidad de la comunicación procediendo a inhabilitar la consulta de registro en la Sede Electrónica en fecha 21 de marzo y con fecha 22 de marzo se realizó una nueva versión que evitaría la vulnerabilidad y que se podría en producción el 26 de marzo de 2019.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 22 de marzo de 2019

ENTIDADES INVESTIGADAS

AYUNTAMIENTO DE MADRID con NIF P2807900B con domicilio en C/ ALCALÁ, 45 - 28014 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 26 de junio de 2019 se remite requerimiento de información al Ayuntamiento de Madrid y de la respuesta recibida se desprende:

Respecto del Ayuntamiento de Madrid

- La aplicación “registro electrónico” se utiliza para el tratamiento de “Registro Electrónico General”, publicado en el Registro de Actividades de

Tratamiento del Ayuntamiento de Madrid y cuyo responsable es la Dirección General de Transparencia, Administración Electrónica y Calidad.

Respecto de la cronología de los hechos y las causas del incidente. Medidas realizadas para minimizar el impacto de la incidencia. Informe de la incidencia

El Ayuntamiento ha aportado copia del informe elaborado por IAM y remitido al Director General de Transparencia, Administración electrónica y Calidad respecto del incidente (Anexo I) del que se desprende:

Cronología de los hechos

- El día 16/03/2019 un ciudadano presenta en el Registro Electrónico del Ayuntamiento de Madrid un escrito en el que informa sobre un incidente de seguridad en una aplicación de la web pública del Ayuntamiento de Madrid.
- El día 20/03/2019, el Responsable del Registro Electrónico reenvía el escrito al IAM el cual contacta con el ciudadano y una vez realizadas las comprobaciones oportunas establece que existe una vulnerabilidad en la consulta de entradas de registro en la Sede Electrónica del Ayuntamiento que permite el acceso a datos personales sin la debida autenticación. (dirección: ******URL.1***)
- El día 21/03/2019, IAM procede a desactivar temporalmente las consultas en el registro hasta que el problema sea corregido.
- El día 22/03/2019 IAM envía toda la información disponible sobre esta vulnerabilidad a la Subdirección General de Administración Electrónica como responsable del tratamiento.
- El día 25/03/2019, el Director General de Transparencia, Administración Electrónica y Calidad, como responsable de la sede electrónica y Delegado de Protección de datos, solicita información adicional sobre este asunto.
- El IAM manifiesta que se ha modificado el código de la aplicación para validar que el acceso al registro solicitado coincida con el usuario que hace la petición web. Se han realizado pruebas y está previsto implantar la nueva versión el 26/03/2019.

Con fecha 1 de octubre de 2019, desde la inspección de Datos se accede a la dirección:
******URL.1***, verificando que el sistema devuelve un mensaje de error.

Asimismo, se comprueba que el acceso a la consulta de registro electrónico solicita una identificación del usuario y genera la dirección: ******URL.2***

Causa del incidente

- El IAM manifiesta que la vulnerabilidad estaba presente debido a una insuficiente aplicación de controles que aseguraran la robustez de la aplicación ya que no se comprobaba que el usuario asociado al apunte del registro coincidiera con el que hacía la petición.
- El IAM manifiesta que no se ha producido una brecha de seguridad. Y declara que el responsable del sistema realiza periódicamente controles sobre la calidad del software de la aplicación y no detectaron este

problema. Tampoco el responsable del servicio ha detectado esta vulnerabilidad en las pruebas de recepción del sistema. Por su parte, el Responsable de Seguridad, encargó la realización de una auditoría de vulnerabilidades en 2015, donde no se encontró la vulnerabilidad.

- El IAM manifiesta que no se puede determinar con certeza la fecha desde la cual la vulnerabilidad estaba presente

Respecto de los datos afectados

- Los datos a los que se podrían acceder son datos personales y documentos aportados por el ciudadano en el registro para realizar la gestión correspondiente.
- El Ayuntamiento manifiesta que no tiene constancia de que la vulnerabilidad haya sido explotada por parte de terceros.
- No se ha realizado ninguna comunicación, ya que no se han detectado posibles afectados.
- Adicionalmente, el 20 de mayo de 2019, IAM envió una carta certificada al ciudadano que informó sobre la vulnerabilidad.

Respecto de las acciones a realizar

- EL IAM manifiesta que el incidente era muy específico y que no parece probable que se den las mismas circunstancias en otros Sistemas de Información del Ayuntamiento, no obstante, se van a realizar las siguientes actuaciones:
    - Realizar de forma urgente una auditoría de vulnerabilidades sobre la sede electrónica del Ayuntamiento.
    - Revisar otras aplicaciones, en busca de vulnerabilidades similares.
    - Se incluirá una referencia a este tipo de vulnerabilidad en la acción formativa de seguridad para los equipos de desarrollo de IAM del Plan de Acción de Seguridad de IAM de 2019.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- El Ayuntamiento de Madrid manifiesta que las medidas más relevantes implantadas con anterioridad al incidente corresponden a:
    - Conexión segura https y canal seguro SSL de comunicación con el ciudadano.
    - Autenticación: por parte de los ciudadanos usando los servicios de Cl@ve y del sistema de identificación de ciudadanos con clave concertada del Ayuntamiento. Por parte del Ayuntamiento exhibiendo el correspondiente certificado,
    - Control de la sesión del usuario,
    - Control de accesos: las diferentes aplicaciones que permiten el acceso de los ciudadanos están diseñadas de tal forma que cada ciudadano solo tenga acceso a su información.

- En la Intranet corporativa figura información sobre violaciones de seguridad con el procedimiento de actuación ante una brecha.

El Ayuntamiento ha aportado una ficha descriptiva del "*Procedimiento de Gestión de Incidentes de Seguridad de la Información en IAM".*

- El Ayuntamiento ha aportado *Acuerdo de la Junta de Gobierno de la Ciudad de Madrid por el que se aprueba la Política de Seguridad e Información del Ayuntamiento de Madrid y sus Organismos Públicos* de fecha 24 de mayo de 2017. Y manifiesta que para el tratamiento de "Registro Electrónico General" se siguen las directrices indicadas en el Acuerdo mencionado.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso, a través de la aplicación de registro del sitio web del Ayuntamiento de Madrid, a datos de terceros ajenos.

No obstante, también consta que el Ayuntamiento de Madrid, a través del servicio de Informática, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido tras una reclamación de un ciudadano la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

También debe valorase la adopción de medidas técnicas y de gestión, como es la contratación de una auditoria a todos los sistemas de información similares, al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a ***AYUNTAMIENTO DE MADRID*** con NIF ***P2807900B,*** y con domicilio en ***C/ ALCALÁ, 45 - 28014 MADRID.***

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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 de la referida Ley.

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