- **Procedimiento Nº: E/07789/2020**

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: Como consecuencia de la notificación a la División de Innovación Tecnológica de la Agencia Española de Protección de Datos (en adelante, AEPD) de una brecha de seguridad de datos personales presuntamente por parte del responsable del tratamiento FUNDACIÓN CAJA GENERAL DE AHORROS DE GRANADA, con número de registro de entrada O00007128e2000003034, relativa a *hacking* en la web de la fundación, la Directora de la AEPD ordenó el 28/09/2020 a la Inspección de Datos que valorase la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

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:

ENTIDADES INVESTIGADAS
Durante las presentes actuaciones se han investigado las siguientes entidades:
FUNDACIÓN CAJA GENERAL DE AHORROS DE GRANADA (en adelante, la investigada), con NIF G18000802

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final:

(…)

Respecto de las causas que hicieron posible la brecha:

(…)

Respecto de los datos afectados:

(…)

Respecto de la notificación de la brecha de seguridad a la AEPD:

(…)

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

(…)

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha de seguridad:

(…)

Respecto de las medidas de seguridad de tipo preventivo frente a la posible repetición en el futuro de la brecha de seguridad:

(…)

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 de disponibilidad

La seguridad del tratamiento viene regulada en el artículo 32, del RGPD.

Artículo 32

"Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a)la seudonimización y el cifrado de datos personales;

b)la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c)la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d)un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

La empresa afirma que previamente a la brecha, contaba con unos servicios especializados en el mantenimiento de la seguridad de los sistemas involucrados en la brecha, aportando copia del contrato. Asimismo aporta copia del RAT y del AR, junto con copias tanto de la política de seguridad como del procedimiento de actuación ante la existencia de una brecha de seguridad. De todo ello se desprende que con anterioridad a la brecha, la entidad investigada disponía de medidas de seguridad razonables

La brecha se produjo por el uso de un malware que aprovecha un agujero de seguridad
en las instalaciones de ******EMPRESA.1*** para a continuación instalar otro plugin que le permite gestionar los ficheros de la parte pública del servidor.

En cuanto al impacto, si bien podrían resultar afectados ******REGISTROS.1.*** La investigada asegura que la brecha se basó exclusivamente en la modificación de la página web, sin que se produjese el acceso a la información almacenada en los archivos privados de la web.

No constan reclamaciones ante esta AEPD por parte de posibles usuarios afectados

Para evitar que estos hechos se vuelvan a repetir se procede a la actualización de todos los plugins que no rompen la web, a la actualización y configuración de un

cortafuegos para ***EMPRESA.1 , así como a la actualización de contraseñas, entre otras medidas.

Hay que señalar que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de notificar a la AEPD, y la rápida adopción de medidas para eliminarla.

Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

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 FUNDACIÓN CAJA GENERAL DE AHORROS DE GRANADA con NIF G18000802

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.

940-0419

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