Procedimiento Nº: E/06443/2019
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 violación de seguridad de datos personales (en adelante quiebra de seguridad) remitido por el Departamento de Derechos Sociales del Gobierno de Navarra, Servicio Navarro de Empleo (en adelante SNE) en el que informan que el 6 de junio de 2019 desde el Servicio Público de Empleo Estatal (SEPE) se detecta un volumen excesivo de llamadas recibidas a su servicio web de consulta de datos de persona física. Desde el SEPE realizan trazas de las llamadas y detectan que proceden de Navarra.

La información accedida corresponde a DNI, nombre y apellidos y el SNE considera que puede haber unos 97500 afectados.

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: 12 de junio de 2019

ENTIDADES INVESTIGADAS

SERVICIO NAVARRO DE EMPLEO - NAFAR LANSARE con NIF Q3150039J con domicilio en C/ GONZALEZ TABLAS, NUM 7 - 31005 PAMPLONA (NAVARRA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 12 de junio de 2019 el SNE notifica a la Agencia Española de Protección de Datos una brecha de seguridad, acompañando un informe en el que ponen de manifiesto lo siguiente:

   Los datos obtenidos por el ataque masivo son el nombre y apellidos de los NIF localizados y en número inferior a los 99.215 de los que han obtenido respuesta.

   Desde el punto de vista de la notificación se ha evaluado utilizando el anexo III de la “Guía para la gestión y notificación de brechas de seguridad” de la AEPD con los siguientes parámetros:

-Volumen: entre 1.000 y 100.000 registros = 3

-Tipología de datos: datos no sensibles = 1

-Impacto: Externo (perímetro atacante) = 6

Total=3x1x6 = 18

Aunque en la guía se recomienda la notificación a la AEPD a partir de 20 puntos se ha decidido notificar a la AEPD ya que en el ataque se han visto afectados el SEPE y el SNE.

Han decidido no avisar a los interesados ya que, dada la naturaleza de los datos, no se considera que haya un alto riesgo para sus derechos y libertades.

2. Con fecha 26 de julio de 2019 la Inspección de Datos solicita a los representantes del SNE información sobre los hechos comunicados a esta Agencia, teniendo entrada escrito de respuesta en el que ponen de manifiesto lo siguiente:

2.1. **Respecto a la cronología de los hechos**

06/06/2019

En torno a las 16:00, desde el Servicio Público de Empleo Estatal (SEPE) se detecta un volumen excesivo de llamadas recibidas a su servicio web de consulta de datos de persona física.

Desde el SEPE se realiza una traza de las llamadas y se detecta que parecen proceder de Navarra.

07/06/2019

A primera hora de la mañana el SEPE corta el acceso al servicio de consulta de datos de persona física, ya que continúan recibiendo un número excesivo de llamadas. Este corte de servicio afecta a todas las comunidades autónomas.

Durante la mañana el SEPE se pone en contacto con la Dirección General de Informática, Telecomunicaciones e Innovación Pública (DGITIP) de Gobierno de Navarra informando del problema.

Desde la DGITIP y el SNE se comienza a investigar las causas del problema.

El SEPE identifica el origen de las llamadas y confirma que una de las direcciones IP de origen es de Gobierno de Navarra

Tras varias paradas, arranques y cortes de servicio para la IP detectada, se restablece el servicio durante el resto de la mañana

A última hora de la mañana, el SEPE decide parar el servicio durante el fin de semana de cara a evitar posibles ataques de denegación de servicio.

10/06/2019

En torno a las 08:30 de la mañana el SEPE restablece el servicio y trabaja con normalidad

Desde la DGITIP y el SNE se continúa trabajando en averiguar el origen del problema.

11/06/2019

La DGITIP identifica que las llamadas enviadas al servicio del SEPE se realizan a través del servicio web EmpleoMovilService. Este servicio web está publicado en Internet, protegido mediante usuario y contraseña, y se utiliza por parte de la app. móvil del SNE.

A las 11:21 el SEPE informa por correo que vuelven a recibirse llamadas masivas desde los servidores de Gobierno de Navarra.

A las 11:27 se corta el servicio EmpleoMovilService, desde la cual se están realizando las llamadas al SEPE, dejando a la app. móvil del SNE sin servicio.

Se identifica que las llamadas proceden de tres direcciones IP ubicadas en USA, Barcelona y Madrid.

En torno a las 12:30 se informa al SEPE que no debería haber problema en recuperar la normalidad en sus servicios, ya que desde las 11:30 se ha cortado la fuente del problema.

Los servicios del SEPE se mantienen operativos, por lo que no hay un impacto en el resto de comunidades autónomas.

En Navarra, salvo la app. móvil (que queda sin servicio al haberse desactivado el servicio web EmpleoMovilService), el resto de las aplicaciones del SNE están funcionando con normalidad.

2.2. **Respecto de las causas que han ocasionado la brecha**

El servicio web EmpleoMovilService está publicado en Internet protegido mediante un usuario y contraseña (modo de seguridad en el transporte con credenciales en el mensaje). Las comunicaciones a través del servicio son seguras (HTTPS). Sin embargo, el usuario y contraseña que se proporcionan a la app. móvil para que invoque el servicio están sin encriptar

2.3. **Respecto de la categoría de los datos afectados**

Los datos obtenidos por el ataque masivo son el **nombre y apellidos de los NIF** localizados y en un número inferior a los 99.215 de los que han obtenido respuesta.

2.4. **Respecto de las acciones tomadas para minimizar la incidencia**

Se ha cortado indefinidamente el servicio EmpleoMovilService, desde la cual se están realizando las llamadas al SEPE, dejando a la app. móvil del SNE sin servicio.

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 los accesos indebidos y disponibilidad, a través de la aplicación web del SNE, a datos de terceros.

No obstante, también consta que el SNE, 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.

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 **SERVICIO NAVARRO DE EMPLEO - NAFAR LANSARE con NIF Q3150039J** y con domicilio en **C/ GONZÁALEZ TABLAS, NUM 7 - 31005 PAMPLONA (NAVARRA)**

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