Expediente Nº: E/07229/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **TELEFONICA DE ESPAÑA S.A.** en virtud de escrito remitido por la propia entidad y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 05/12/2017, tuvo entrada en esta Agencia escrito de la representación de TELEFONICA DE ESPAÑA S.A. (en lo sucesivo TELEFONICA) por los siguientes hechos: notificación el 05/12/2017 de una quiebra de seguridad.

Las actuaciones de inspección se inician por la recepción de un escrito remitido por TELEFONICA en el que notifican que, con fecha 26/11/2017, han tenido conocimiento de una vulnerabilidad que afectaba al servicio de *Telefónica Centrex IP*, servicio del segmento empresas que consiste en una centralita virtual contratada por el cliente adicional a la prestación del servicio de telecomunicaciones y que permite gestionar las llamadas de las líneas corporativas. Una vez detectada la vulnerabilidad, TELEFONICA activo el protocolo de seguridad y desde el día 27 de noviembre se encuentra corregido el fallo de seguridad.

El equipo técnico de TELEFONICA, después de realizar un análisis forense, ha puesto de manifiesto que la brecha de seguridad no ha afectado a datos personales, ya que es un servicio de empresas y, en todo caso, afectaría a datos de nombre y apellidos de los empleados de las empresas que tiene asignadas extensiones corporativas.

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:

Con fechas 19 y 20/02/2018 se recibe escrito de contestación de TELEFONICA (definido por el operador como CONFIDENCIAL) al requerimiento de información remitido desde la Inspección de Datos en fecha 17/01/2018, en el que se pone de manifiesto:

1. *Centrex IP* es una solución de comunicación corporativa avanzada que permite la creación de un servicio de red privada virtual de voz utilizando una nueva tecnología (servicios de voz sobre red IP) como infraestructura de soporte de servicio (centralita virtual, exclusivo para clientes empresas que evita instalar equipos en la sede del cliente)

   Centrex IP permite integrar todas las sedes de una empresa en una única red de voz, similar a una centralita privada sin restricciones de localización así como crear una red de voz de multidependencia.

   El servicio se presta sobre una plataforma que permite gestionar y configurar la numeración de teléfonos corporativos.

   Para la instalación, gestión y configuración de *Centrex IP* hay disponibles dos portales:

PORTAL DE GESTIÓN DE GRUPOS (PGG): ENTORNO WEB DE GESTION QUE PERMITE EJECUTAR DISTINTAS ACTIVIDADES PARA EL PERSONAL DE TELEFÓNICA. DE ACCESO MEDIANTE USUARIO Y CONTRASEÑA.

EXTERNAL WEB SERVICES (EWS): ENTORNO WEB PARA CLIENTES-EMPRESA PARA LA GESTION. DE ACCESO MEDIANET USUARIO Y CONTRASEÑA

2. En fecha 27/11/2017 a las 22:19, el Centro Especializado en Tecnologías de la Información de Telefónica recibe una notificación de una incidencia en la que se pone de manifiesto que un cliente de la compañía ha informado al Instituto Nacional de Ciberseguridad (INCIBE) de la existencia de una vulnerabilidad en un portal del servicio *Centrex IP.* Y en esa misma fecha, el equipo de Telefónica descubre que la vulnerabilidad está relacionada con el portal PGG en el acceso al perfil de administrador.

3. En fecha 28/11/2017 a las 10:00 se cambian todas las contraseñas de todos los usurarios administradores de Telefónica con acceso al portal.

   Asimismo se implantan medidas de filtro y bloqueo para prevenir ataques en ambos portales, y se realizan diversas acciones sobre el portal PGG antes de volver a poder ser utilizado.

4. Con fecha 04/12/2017, se analizan los accesos no habituales, detectándose 12 direcciones IP desde redes de anonimato (TOR) y desde otro operador (los accesos de los clientes se realizan desde redes de Telefónica).

   Telefónica manifiesta que estos accesos no autorizados no se han producido por una política de contraseñas no robusta o por algoritmos débiles.

5. El número de clientes-empresas afectados ha sido de un total de treinta y uno.

6. Respecto de los datos accesibles al portal PGG, Telefónica manifiesta que no se ha visto afectado ningún dato personal y la información que figura corresponde a datos de la empresa-cliente, identificadores de usuarios de la aplicación del portal, información sobre teléfonos corporativos (números, tipos, grupos, y extensiones). Tendría únicamente datos de las personas físicas que prestan sus servicios en las empresas.

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 (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

El artículo 9.1 de la LOPD establece que:

"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".

Y el artículo 10, relativo al deber de secreto, establece que:

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

En el presente caso, es de destacar que haya sido la propia entidad la que el 05/12/2017 ha notificado a la Agencia una vulnerabilidad en el servicio *Telefónica Centrex IP,* registrando la misma y, que una vez detectada se actuó con diligencia corrigiendo el fallo inmediatamente al activarse los protocolos correspondientes.

De la información aportada y de la recabada por los servicios de inspección en fase de actuaciones previas, se desprende que el contenido de la información de los citados dispositivos se halla totalmente protegida al ser cambiadas todas las contraseñas de acceso, implantándose medidas de filtrado y bloqueo para prevenir posibles ataques, llevándose a cabo actuaciones encaminadas a determinar posibles vulnerabilidades antes de volver a su uso, minimizando los efectos de la quiebra sin que se tenga constancia de que terceros no autorizados hayan accedido a la información

TELEFONICA manifiesta que no se ha visto afectado ningún dato personal y que la información que figura corresponde a datos de la empresa-cliente, identificadores de usuarios, teléfonos corporativos, etc., y que

únicamente contendría datos de las personas físicas que prestan sus servicios en las empresas.

Hay que señalar que el artículo 2 del Reglamento de desarrollo de la LOPD excluye del ámbito de aplicación de la LOPD determinados datos de carácter personal entre los que se encuentran los relativos a personas jurídicas y personas de contacto, es decir, aquellos ficheros que se limiten a incorporar datos de personas físicas que prestan sus servicios en aquellas consistentes únicamente en su nombre y apellidos, funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y fax profesionales, si bien dicha exclusión se halla justificada en la medida en que son necesarios para mantener la relación con la persona jurídica, pero fuera de estos casos cualquier tratamiento que contuviera datos adicionales a los citados o que tuviera una finalidad distinta a la de mantener la relación con la persona jurídica, se encontraría plenamente sometido a la LOPD.

Por ello resultan de aplicación a los ficheros analizados las previsiones contenidas en el Título VIII del RLOPD, relativo a las medidas de seguridad que deben implantarse en el tratamiento de datos de carácter personal, pues contienen datos de personas físicas que podrían resultar comprometidos si se producen accesos no autorizados.

A este respecto, la Sentencia de la Audiencia Nacional de 25/06/2015 ha señalado lo siguiente: *"En interpretación del citado artículo 9, esta Sala ha señalado en múltiples sentencias, (SSAN, Sec. 1ª, de 13 de junio de 2002, Rec. 1517/2001; 7 de febrero de 2003 Rec. 1182/2001; 25-1-2006 Rec. 227/2004; 28 de junio de 2006 Rec. 290/2004 etc), que la obligación que dimana del mismo no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, toda responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica".*

En el presente caso, resulta destacable la diligencia observada por parte de la entidad tras detectarse la vulnerabilidad producida registrando la incidencia, notificando la misma a la Agencia, gestionando y actuando con diligencia activando los protocolos correspondientes y adoptando medidas oportunas para evitar y prevenir hechos similares.

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **TELEFONICA DE ESPAÑA S.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.

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