- **Procedimiento Nº: E/00712/2020**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha de 28 de enero de 2020 la Directora de la Agencia Española de Protección de Datos acodó iniciar actuaciones de investigación ante la notificación a esta Agencia de la indexación en buscadores de internet de datos personales desde servidores del GRUPO SOLIVESA.

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 notificación, por las que tuvo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de entrada de la comunicación: 24 de enero de 2020

ENTIDADES INVESTIGADAS

El GRUPO SOLIVESA, con domicilio en Av Juan Gil Albert 1, Planta 7º, 03804 Alcoy (Alicante) en calidad de encargada del tratamiento. Este grupo está formado, entre otras, por:

- SOLIVESA MASTER FRANCHISE, S.L., con CIF B97154488 y domicilio en Calle Salamanca 60, piso 3, Planta 7, 46005 Valencia. En calidad de encargada del tratamiento.
- VESALEADS, S.L., con CIF B40508731 y domicilio en Calle Salamanca 60, piso 3, Planta 7, 46005 Valencia. En calidad de encargada del tratamiento.
- VODAFONE ESPAÑA, S.A.U. con NIF A80907397 y con domicilio en Avenida de América 115, 28042 Madrid. En calidad de responsable del tratamiento.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

El día 24 de enero de 2020 tuvo entrada en los buzones de correo electrónico del departamento Internacional y el departamento de Unidad Tecnológica de la Agencia Española de Protección de Datos (AEPD) un mensaje remitido por un ciudadano y dirigido, además de estas citadas unidades de la AEPD, a otras direcciones de correo electrónico del grupo Solivesa en el que se comunicaba lo siguiente en lengua inglesa: *“Hemos encontrado casualmente una gran vulnerabilidad en los servidores del Grupo Solivesa. Google está indexando contenido privado. Esto es muy problemático ya que el contenido que se almacena es muy privado (tarjetas de identidad personal, registros bancarios, contratos, direcciones y números de teléfono). El robo de identidad es ALTAMENTE PROBABLE.*

*Al buscar en Google la IP *****IP.1**, obtenemos algunos resultados. El servidor Apache está indexando cada directorio. Cualquiera puede acceder a TODA la información.*

'https://east.gruposolivesa.com' tiene una subcarpeta llamada 'uploads' también está indexada y publicando el contenido.

Se adjunta un zip cifrado que contiene algunos ejemplos extraídos de los directorios PÚBLICOS, como prueba."

El correo electrónico anexa la siguiente documentación:

- Impresión de pantalla del resultado de la consulta en el buscador de Google con el criterio "*site: *****IP.1**".*
- Impresión de pantalla del contenido de la carpeta "*uploads*" en la que se observa que contiene 45 documentos con formatos *pdf* e imágenes *"denominados con nombres como CIF, DNI, Recibo, factura, etc…*".
- Copia de algunos de estos documentos como la imagen de un DNI y dos ficheros con formato de hoja de cálculo Excel que contienen ******REGISTROS.1*** y ******REGISTROS.2*** registros respectivamente con datos personales correspondientes a nombre y apellidos, número de teléfono y una serie de parámetros técnicos de la portabilidad gestionada.

Con fecha 30 de enero de 2020 se solicitó información al DPD de Grupo Solivesa, y, con fecha 12 de febrero de 2020, tuvo entrada un escrito de respuesta en el que se manifiesta lo siguiente:

Respecto al Grupo Solivesa:

GRUPO SOLIVESA está constituido por las sociedades SOLIVESA MASTER FRANCHISE, S.L y VESALEADS, S.L. Estas sociedades comercializan los servicios de telefonía y actúan como encargadas del tratamiento de VODAFONE ESPAÑA, S.A.U, según figura en el contrato de encargo de tratamiento.

Respecto a la cronología de los hechos:

El viernes 24 de enero de 2020 se recibió en Grupo Solivesa un correo electrónico que informaba de la existencia de una brecha de seguridad en los sistemas de Grupo Solivesa. En ese mismo instante se activó el protocolo de respuesta ante brechas de seguridad definido por el Grupo Solivesa.

Revisados los sistemas de seguridad implementados en Grupo Solivesa, no se detectó ningún acceso a servidores, bases de datos o recursos con carácter anormal o que se pudiera identificar como un acceso no autorizado.

Examinada la información que se adjunta en el correo electrónico y los pasos seguidos por el informante, se observó que este ha obtenido la información directamente desde los servicios de búsqueda y caché de páginas de Google y no por un acceso indebido a recursos del Grupo Solivesa. El correo adjunta varias capturas de pantalla donde en algún caso se aprecia información de carácter personal.

Al detectar la brecha de seguridad el día 24/01/2020 se hizo una primera notificación a VODAFONE ESPAÑA S.A.U dentro de las 24 horas siguientes a tener conocimiento de la misma de acuerdo con el procedimiento que se indica en el contrato de encargo de tratamiento firmado entre las empresas de GRUPO SOLIVESA y VODAFONE ESPAÑA S.A.U. (en adelante, Vodafone) del cual aportan copia.

El día 25/01/2020, el DPD y los responsables de VODAFONE convocaron el día 28/01/2020 a una reunión telefónica a los responsables de Grupo Solivesa, los responsables informáticos de la empresa, la empresa de ciberseguridad y el DPD de Grupo Solivesa. Después de esta reunión remitieron el informe de gestión de la brecha de seguridad redactado con fecha 26/01/2020 que les aporta la empresa de ciberseguridad de GRUPO SOLIVESA (Vibranium Tecnología Viva S.L). Este informe es el mismo que adjuntaron a la contestación del requerimiento de la AEPD en el que se certifica por parte de la empresa Vibranium Tecnología Viva S.L que solo se ha podido acceder a información de unos ******REGISTROS.3*** registros a través de directorios indexados en Google. El día 05/02/2020 se comprobó que ya no hay contenido indexado en Google, por lo que se dio por cerrada la brecha de seguridad. A fecha de 12/02/2020 VODAFONE les comunica que han archivado la incidencia y que no consideran que sea necesario notificar la brecha a la AEPD. Aportan copia de la ficha de registro de la incidencia y cierre de la misma.

En el momento de redactar el informe de Inspección, se realizaron los mismos accesos llevados a cabo por el supuesto atacante y se comprobó que Google no tiene en caché ninguna información cuyo *site* sea el indicado. Asimismo, el acceso al servidor o servicios a través de esta URL son infructuosos. Se realizó el acceso a la carpeta "*uploads*" indicada en el correo, con idéntico resultado negativo.

Respecto al volumen y tipo de datos afectados

Compruebaron que en las URLs manifestadas por el informante se obtuvieron ******DOCUMENTOS.1*** documentos con formato de Excel, que una vez analizados se observó que contienen unos ******REGISTROS.3*** registros con los siguientes datos de carácter personal: nombre, apellidos, número de teléfono, dirección y última portabilidad.

Los datos indexados en Google correspondían a Leads (solicitudes de información a través de web) de clientes potenciales de Vodafone.

Identificación de las causas que originaron la fuga:

Una vez analizados y considerados los datos recogidos, concluyeron que no ha habido una amenaza directa contra la infraestructura, recursos o información albergada en las instalaciones que soportan la información del Grupo Solivesa.

La información recogida y comunicada por el informante, se ha obtenido desde una serie de páginas antiguas indexadas en el caché del buscador Google.

Se ha recogido toda la información relativa a la "brecha de seguridad", aunque no ha habido ninguna afectación a infraestructura, recursos o servicios del Grupo Solivesa. Hay información supuestamente extraída por los *crawler* (programa que analiza los

documentos de los sitios web) del buscador Google e indexada en un tiempo pasado (agosto 2019).

La clasificación corresponde con una “brecha de confidencialidad”.

En el estudio técnico y análisis forense previo, se concluye que es posible que en procesos de migración o movimiento de datos en el servidor y en un momento puntual quedó expuesto, donde el *crawler* de Google haya podido acceder a un número pequeño de información que almacenaba dicho servidor.

Este servidor indicado no está en producción desde el pasado mes de agosto de 2019. En el momento actual, no es posible determinar cuándo fue el momento exacto y como se pudo producir la entrada del *bot* de indexación del buscador Google en el servidor web (Googlebot).

Respecto a las acciones tomadas para la resolución de la brecha

Desde el conocimiento del incidente el 24/01/2020, se ha procedido a la revisión exhaustiva por parte de los técnicos del Grupo Solivesa y de un técnico experto en seguridad externo de toda la infraestructura, recursos y servicios de Grupo Solivesa, y se concluyó que no ha habido en los últimos meses, ningún acceso no autorizado a dichos recursos o servicios.

Se ha solicitado a través de los medios que pone al alcance la empresa Google, la eliminación de las páginas indexadas en su buscador, correspondientes con la IP ******IP.1*** a través de su herramienta “Google Search Console” para sitios web.

Respecto de si se tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través del ataque

No se tiene conocimiento de que haya personas que estén utilizando datos personales obtenidos a través de los contenidos indexados en Google. La única persona de la que consta que ha tenido acceso al contenido indexado en Google es la persona anónima que informó sobre la brecha de seguridad**.**

Respecto de la notificación realizada a los clientes afectados

Con fecha 25/01/2020 se informó de la brecha de seguridad al Responsable del Tratamiento, VODAFONE, para que decidiera si era necesario notificar a la AEPD y comunicar a los interesados. El día 12/02/2020 VODAFONE comunicó que han decidido no notificar la brecha de seguridad a la AEPD ni comunicar a los interesados por su escaso nivel de riesgo.

Respecto de la seguridad de los tratamientos de datos con anterioridad a la incidencia de seguridad

Adjuntan Copia del Registro de Actividad de este tratamiento tanto de VESALEADS, S.L como de SOLIVESA MASTER FRANCHISE, S.L.

Hay registrada una actividad de tratamiento correspondiente a Leads que se siguen generando y que se almacenan en unos nuevos servidores de la empresa 1&1 IONOS ESPAÑA S.L.U.

El Análisis de Riesgo de las actividades de tratamiento donde se ha producido la brecha no se pudo realizar ya que no se tenía constancia de que hubiera contenido indexado en Google a través del servidor que no estaba en producción desde agosto de 2019. Disponen el resto del análisis de riesgos realizados.

Aportan copia del procedimiento establecido de brechas de seguridad en VESALEADS, S.L y SOLIVESA MASTER FRANCHISE, S.L. Aunque la brecha de seguridad ha sido gestionada conjuntamente por las dos empresas, cada empresa tiene establecido el mismo procedimiento de gestión de brechas de seguridad.

Aportan la política de seguridad establecida tanto en VESALEADS, S.L como en SOLIVESA MASTER FRANCHISE, S.L. Ambas políticas de seguridad coinciden y los tratamientos que se realizan son los mismos.

Se incluye la relación de las medidas de seguridad específicas para el tratamiento de <OBTENCIÓN Y ALMACENAMIENTO DE LEADS>, en el propio registro de actividad de este tratamiento.

Con fecha 26 de marzo de 2020 se han realizado comprobaciones por la Inspección de Datos de la AEPD en el buscador de GOOGLE con los criterios de búsqueda: “Site: 178.62.219.113” y se ha accedido a la siguiente url:

<***URL.1*** >, no se ha encontrado información con datos de carácter personal.

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, la violación de la seguridad notificada a través de un email anónimo tuvo como consecuencia una vulnerabilidad de la confidencialidad al permitir

al público en general el acceso a información supuestamente extraída por los *crawler* (programa que analiza los documentos de los sitios web) del buscador Google e indexada en un tiempo pasado (agosto 2019).

El contenido de la información a la que se ha tenido acceso se refiere a nombre, apellidos, dirección postal y teléfono de potenciales clientes de Vodafone que habían solicitado portabilidad hasta agosto de 2019.

Al objeto de minimizar el impacto sobre los interesados, el Grupo Solivesa solicitó a través de los medios que pone al alcance la empresa Google, la eliminación de las páginas indexadas en su buscador, correspondientes con la IP ******IP.1*** a través de su herramienta "Google Search Console" para sitios web.

Con fecha 5/02/2020, una vez comprobada la imposibilidad de acceder de nuevo por los bot de Google (Googlebot) se procedió a cerrar las actuaciones y dar como finalizada la brecha de seguridad notificada.

No consta que haya habido tratamientos posteriores de los datos afectados por la brecha de seguridad y no constan reclamaciones al respecto ante esta AEPD por los interesados.

El Grupo Solivesa dispone de Registro de tratamientos y análisis de riesgos de los tratamientos afectados en la brecha de seguridad.

En consecuencia, se aprecia un nivel de diligencia proporcional y razonable en la actuación de la entidad Grupo Solivesa como encargada de los tratamientos y Vodafone como responsable de dichos tratamientos, en función de las medidas de seguridad previas implantadas al incidente sobrevenido, así como en la corrección de las disfuncionalidades notificadas respecto a los accesos indebidos como consecuencia del almacenamiento temporal de logs y su posterior recuperación a través de bots de Google.

Cabe señalar, por último, que 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, consta que la actuación del Grupo Solivesa (encargada del tratamiento) y de Vodafone (responsable del tratamiento), ha sido diligente y proporcional con la normativa sobre protección de datos personales analizada en los párrafos anteriores al corregir y minimizar el impacto de la brecha de seguridad sobre los interesados.

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: VODAFONE ESPAÑA, S.A.U. con NIF A80907397 y con domicilio en Avenida de América 115, 28042 Madrid. En calidad de responsable del tratamiento.

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