- **Procedimiento Nº: E/11184/2019**

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 iniciaron por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por ***A.A.A.*** (en adelante, notificante) en el que informa a la Agencia Española de Protección de Datos (en adelante, AEPD) de que, con fecha 29 de octubre de 2019, al ir a sustituir el disco externo de la copia de seguridad de la asesoría fiscal de la notificante, detectan que el disco externo que contenía una copia anterior fue robado al encontrarse abierta una ventana que permitía el acceso parcial al interior del local.

Aportan en la notificación, denuncia interpuesta ante la Dirección General de la Policía de Tenerife, en fecha 29 de octubre a las 12:03 horas, donde se pone de manifiesto que la Asesoría Fiscal se encuentra en la planta baja y al estar la ventana abierta le sustrajeron el dispositivo de memoria externa que se encontraba conectado a un ordenador personal ubicado junto a la ventana aunque no hay testigos de este hecho. Dicho dispositivo contiene datos personales y profesionales de sus clientes. También se pone de manifiesto que disponen de cámaras de videovigilancia que se activan fuera de los horarios de la Asesoría.

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, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de los datos personales: 30 de octubre de 2019

ENTIDADES INVESTIGADAS

A.A.A. con NIF ******NIF.1*** y con domicilio en ******DIRECCION.1*****.**

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 27 de noviembre de 2019 se solicitó información al notificante y de la respuesta recibida en fecha 18 de diciembre se desprende lo siguiente:

Respecto de la cronología de los hechos. Medidas de minimización del impacto de la brecha de seguridad.

El día 28 de octubre de 2019 sufrieron el robo de un disco duro por un desconocido a través de una ventana abierta del local.

- La titular de la Asesoría Fiscal (notificante) manifiesta que inmediatamente se comunicó la incidencia al técnico informático quien comprueba los posibles daños tanto en el ordenador como en las copias de respaldo, y se verifica que no ha habido pérdida de datos.

Los datos fueron recuperados no viéndose alterada la disponibilidad ni la integridad. También se pone en conocimiento los hechos a la consultoría que les presta servicio de asesoramiento en protección de datos y se presenta denuncia ante la Policía.

Respecto de las causas que hicieron posible la brecha de seguridad.

- En horario laboral el disco duro se encontraba en funcionamiento y fue sustraído del cable que lo mantenía conectado al ordenador utilizando la fuerza de forma sorpresiva para los trabajadores
- La policía no ha podido localizar el dispositivo ni a la persona que lo ha sustraído. Tampoco el Ayuntamiento ha encontrado el dispositivo.

Respecto de los datos afectados.

- El disco duro contenía los datos de 154 clientes
- Los datos corresponden a las declaraciones de la renta de los clientes: Datos básicos y de contacto, datos económicos y financieros. En algún caso también había datos de salud por baja médica y excepcionalmente datos de filiación política.
- El dispositivo dispone de claves de acceso al contenido.
- Se ha comunicado electrónicamente la brecha a los clientes en fecha 10 de diciembre previo mandato de la Directora de la AEPD de fecha 21 de noviembre de 2019 y se ha habilitado un correo para las posibles dudas de los clientes.

A este respecto, se ha aportado Resolución de la AEPD que ordena la comunicación de la brecha a los interesados y copia del escrito a los clientes donde se informa de la sustracción de un disco duro que ha provocado una posible divulgación no autorizada de datos de carácter personal y se pone a disposición de los clientes la dirección ******EMAIL.1*** para las dudas o comentarios que quieran transmitir y desde la que se dará una respuesta personalizada. No tiene constancia de la utilización posterior de los datos sustraídos ni de su publicación en Internet.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha de seguridad.

La notificante manifiesta que el disco duro disponía de un sistema de cifrado que se activa en el momento de ser desconectado del ordenador. Fuera del horario laboral el dispositivo se custodia en un archivo cerrado con llave dentro de una habitación cerrada con llave y de acceso únicamente al personal autorizado. En el escrito de contestación se han aportado fotografías del armario donde se custodian los archivos y la puerta de la habitación de acceso, ambas con cerradura con llave.

- El local dispone de rejas y persianas que normalmente no se abren. La notificante manifiesta que se abrieron puntualmente debido a una oleada de calor. Se ha aportado fotografía de la reja y la ubicación del ordenador.
- En el escrito de contestación se han aportado los siguientes documentos:

    o Registro de actividad
    o Política de gestión de brechas
    o Política de seguridad
    o Registro de incidencias

Respecto de las medias implementadas con posterioridad la brecha de seguridad.

- Se está valorando la instalación de verjas en todas las ventanas.
- Se está valorando eliminar las copias de seguridad físicas.
- Se ha contratado un servicio de almacenamiento en nube.
- Se va a realizar un taller formativo para los trabajadores encaminado a fomentar de forma segura el tratamiento de datos y la importancia de gestión de brechas 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

En el presente caso, consta que con anterioridad a la brecha de seguridad se tenían implantadas medidas de seguridad razonables en función de los posibles riesgos estimados. Así, la copia de seguridad de los ordenadores del personal trabajador se custodiaba bajo llave en un armario. Solo disponían de las llaves de acceso el personal autorizado. El soporte sustraído estaba encriptado y con clave de acceso, según consta en los protocolos de seguridad a fecha del incidente.

Consta también que disponían de Registro de actividad, Política de gestión de brechas, Política de seguridad y Registro de incidencias.

En cuanto a las medidas adoptadas para minimizar el impacto del incidente, cabe señalar que se procedió a valorar la instalación de verjas en todas las ventanas y eliminar las copias de seguridad físicas, se ha contratado un servicio de almacenamiento en nube y se va a realizar un taller formativo para los trabajadores encaminado a fomentar de forma segura el tratamiento de datos y la importancia de gestión de brechas de seguridad.

Por mandato de la Directora de la AEPD se procedió, tras la notificación de la brecha de seguridad de los datos personales, a comunicar a los afectados de la incidencia a través de correo electrónico y se ha puesto a disposición de los mismos un formulario para las dudas o comentarios que quieran transmitir y desde la que se dará una respuesta personalizada.

En consecuencia, acaecido el riesgo de desaparición del soporte, en lo sucesivo deberá contemplarse riesgos similares, incluida la posible actuación por sabotaje interno, por lo que la obligación establecida de encriptación total de los datos tanto en los ordenadores personales como en los soportes de copias de seguridad parece suficiente para evitar situaciones como la ahora analizada que ha originado una supuesta vulneración de la confidencialidad y siempre que la clave de encriptación se encuentre debidamente custodiada y para su acceso se requiera al menos dos autorizados.

Por último, no consta hasta la fecha que los datos personales contenidos en el soporte hayan sido objeto de tratamiento posterior y ni constan reclamaciones de los afectados.

III

Por lo tanto, la actuación del notificante, como entidad responsable del tratamiento, ha sido proporcional 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 ***A.A.A.*** con NIF ******NIF.1*** y con domicilio en ******DIRECCION.1*.**

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