Procedimiento Nº: E/07413/2019
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: Con fecha de 30 de julio de 2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a una brecha de seguridad notificada por la asociación ACCEM sin ánimo de lucro y declarada de utilidad pública, relativa a la pérdida de un dispositivo de almacenamiento conteniendo datos de carácter personal.

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 la brecha de seguridad: 23 de julio de 2019

ENTIDADES INVESTIGADAS

ACCEM con NIF G79963237 con domicilio en PLAZA SANTA MARIA SOLEDAD TORRES ACOSTA, 2 PISO 3 - 28004 MADRID.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Sobre ACCEM

Según la información obrante en su página web ACCEM es una asociación sin ánimo de lucro declarada de utilidad pública y registrada en el Ministerio del Interior con el nº 97.521. Es una organización de ámbito estatal cuya misión es la defensa de los derechos fundamentales, la atención y el acompañamiento a las personas que se encuentran en situación o riesgo de exclusión social. Especializada en refugio y migraciones para la inclusión de las personas.

El equipo profesional de ACCEM lo conforman 1.441 personas a 30 de junio de 2019. Además, un total de 858 personas realizan actividades de voluntariado con la entidad (dato total 2018).

Desde 2012, ACCEM es Agencia de Colocación Estatal con 25 centros, autorizada por el Servicio Público de Empleo Estatal dependiente del Ministerio de Empleo y Seguridad Social, con número de agencia 9900000144.

Respecto a los hechos

ACCEM ha comunicado a esta Agencia los siguientes hechos en la notificación de la brecha de seguridad:

En la mañana del 22 de julio de 2019 la responsable de la sede en Vitoria comunicó la detección de la ausencia de un disco duro externo que custodiaba en su despacho que contenía una copia de seguridad de los ordenadores del personal de la sede. Informan de la interposición de denuncia ante la Policía.

El disco duro externo se encontraba en un armario cerrado con llave al que sólo tenía acceso la responsable provincial, la responsable territorial y la administrativa de la sede (persona encargada de las llaves en ausencia de la responsable provincial).

El armario a su vez estaba en el despacho de la responsable provincial, despacho que en ausencia de la responsable permanece cerrado y del que sólo tienen las llaves las mismas personas que las indicadas en el párrafo anterior.

La responsable cierra de forma habitual tanto el armario como el despacho y no se explica cómo ha podido desparecer el disco duro. La cerradura del armario y la cerradura del despacho no estaban forzadas, por lo que se atribuye la desaparición a algún posible despiste que haya podido tener la responsable en algún momento en el que haya abandonado el despacho sin cerrarlo ni cerrar el armario (por ejemplo, para ir al baño o para recoger documentación en la impresora).

ACCEM ha informado que la brecha puede haber afectado a unas 240 personas en total, entre usuarios del programa de protección internacional y personal de la sede. Solo estaba cifrada la información relativa al personal. Las categorías de datos afectadas son: datos básicos, datos identificativos, de contacto, económico-financieros, de salud, sobre religión o creencia, sobre origen racial sobre opinión política, y sobre vida sexual. Contenía informes psicológicos de 100 de los afectados.

Respecto a las medidas implementadas con anterioridad a la brecha:

ACCEM ha aportado a requerimiento de la Inspección de Datos la siguiente información y documentación:

- Con respecto las políticas y medidas de seguridad generales:

  ACCEM ha aportado copia del **Registro de Actividades de Tratamiento**, en el que se verifica constan actividades tales como la realización de informes psicológicos y de acogida con las finalidades de orientación psicológica y gestión de asistencia social. También aparece una actividad de tratamiento de gestión administrativa.

  Aportan copia del **Análisis de Riesgos** para la sede de Euskadi, que se verifica se encuentra fechado el 30/01/2019.

Indican que no se ha estimado necesaria la realización de una **Evaluación de Impacto** sobre la actividad realizada en la sede de ACCEM en Vitoria debido a los siguientes motivos:

- El Programa de Protección Internacional y la actividad de la sede no han sufrido variaciones desde la entrada en vigor del Reglamento en cuanto al tratamiento de datos personales.
- En la sede de ACCEM en Vitoria se ha atendido a 240 personas aproximadamente desde su apertura, por lo que, aunque parte de los datos tratados son datos sensibles, no estamos ante un tratamiento de datos a gran escala.
- Si bien del análisis de riesgos realizado en la sede de ACCEM en Vitoria se deriva que existe un cierto riesgo por la falta de medios informáticos, se han tomado medidas de seguridad provisionales hasta la instalación del nuevo servidor. Debido a que el riesgo existente no se estimaba alto, no se consideró necesario hacer una evaluación de impacto tal y como se recoge en el análisis de riesgos.

- En cuanto a las medidas de seguridad adoptadas aportan copia del del Manual de Seguridad de ACCEM de fecha 07/02/2019, que era la versión del Manual vigente en el momento en el que se produjo la brecha de seguridad, en el que se detallan todas las medidas de seguridad llevadas a cabo por la entidad.

  Las medidas de seguridad eran las siguientes:

- MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE FICHEROS.

  - Condiciones de acceso para el personal ajeno.
  - Continuidad del servicio.
  - Identificación de soportes y documentos.
  - Entrada y salida de soportes y documentos.
  - Gestión de incidencias de seguridad.
  - Funciones y obligaciones del personal.
  - Auditorías.

- MEDIDAS ESPECÍFICAS PARA FICHEROS Y TRATAMIENTOS MANUALES.

  - Control de acceso físico.
  - Registro de accesos a la documentación.
  - Criterios de archivo.
  - Mecanismos de protección.
  - Ubicación de los dispositivos de almacenamiento.
  - Desecho de documentos.
  - Custodia de documentos.
  - Gestión de los soportes que almacenan documentos y traslado de documentos.

- MEDIDAS ESPECÍFICAS PARA FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

  - Acceso a datos a través de redes de comunicaciones.
  - Protección de las redes de comunicaciones internas.
  - Ficheros temporales y copias de trabajos de documentos.
  - Identificación y autenticación.
  - Alta de usuarios.
  - Baja de un usuario.
  - Modificación de permisos de un usuario.
  - Reactivación de usuarios.
  - Registros.
  - Asignación de identificadores y contraseñas personales por cada usuario.
  - Distribución y comunicación de las contraseñas.
  - Gestión de contraseñas.
  - Control de acceso.
  - Registro de accesos.
  - Pruebas con datos reales.
  - Régimen de trabajo fuera de los locales del responsable.
  - Cifrado en la distribución o salida de soportes automatizados de datos.
  - Copias de respaldo y de recuperación.

  Indican que existen PROCEDIMIENTOS DE REVISIÓN DEL CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD.

- Con respecto a las medidas de custodia de los equipos informáticos y soportes que almacenan datos en las oficinas en la sede de ACCEM en Vitoria en el momento de la brecha:

  - **Sólo accede a la oficina el personal de ACCEM y si acceden personas usuarias de los Programas, lo hacen en todo momento bajo supervisión del personal de ACCEM** con el que han concertado una entrevista o, en caso de acudir a la sede a solicitar información, bajo la supervisión de la persona encargada en ese momento de la recepción.

  - La oficina tiene seguridad en los accesos físicos **con llave** (adjuntan fotos de estas comprobándose que están dotadas de cerradura). La puerta en horario de apertura se vigila por la persona encargada de la recepción (el personal se turna para realizar esta función).

  - Fuera del horario de apertura los accesos se cierran y sólo tienen las llaves de acceso a la oficina las personas autorizadas (responsable provincial, responsable territorial y administrativa de la sede).

  - No hay ordenadores portátiles, los ordenadores son de sobremesa y cada empleado de la sede tiene asignado el suyo.

En el momento de la brecha la información se guardaba en el ordenador asignado a cada trabajador/a y sólo él/ella tenía acceso de forma individual con su usuario y contraseña y el responsable de informática cómo administrador. El responsable de informática tenía la posibilidad de conectarse desde la Sede Social de ACCEM en remoto para resolver incidencias.

En la actualidad se ha instalado un equipo en el que se guarda toda la información (ya no se guarda información en los equipos individuales) y que dispone de un esquema de permisos de acceso. El equipo de almacenamiento se custodia permanente al que sólo tienen acceso el responsable provincial, la responsable territorial y la administrativa de la Sede.

- No hay USB ni dispositivos portátiles en los que se extraigan datos fuera de la sede, sólo existía un disco duro externo dónde se realizaba semanalmente la copia de seguridad de todos los ordenadores de la sede y **que se custodiaba en un armario bajo llave ubicado en el despacho de la responsable provincial, que a su vez se cierra con llave y que está ubicado en la propia sede** (adjuntan fotografías). Actualmente se ha adquirido otro equipo externo en sustitución del desaparecido y las copias de seguridad se realizan tanto en el servidor como en el disco duro externo y se encriptan.

- La psicóloga, la administrativa y la responsable provincial tienen sus equipos en despachos que se cierran con llave, el resto de equipos se encuentran en el espacio común vigilados en todo momento por el personal de ACCEM.

- Los archivos físicos se custodian parte en una habitación bajo llave que se usa como archivo, parte en armarios bajo llave en el espacio común y parte que contienen datos del personal que se guardan en los despachos de la administrativa y la responsable provincial y los de la psicóloga. Todos estos archivos se encuentran dentro de armarios bajo llave. Las llaves de los despachos de administración y del despacho de la responsable provincial las tienen la responsable provincial, la responsable territorial y la administrativa y la llave del despacho de psicología la tiene la psicóloga, la responsable provincial y la responsable territorial.

- Los documentos de trabajo temporal se guardan durante la jornada en cajoneras bajo llave. Las llaves de cada cajonera las tiene el/la empleado/a que la tiene asignada y otra copia la custodia la responsable provincial. Al finalizar la jornada toda la documentación se lleva al archivo.

En cuanto a las directrices de encriptación de Accem las mismas se localizan en los siguientes puntos de la versión 03 del Manual de Seguridad:

- 6.4 Entrada y salida de soportes y documentos.

  "(…) La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos

datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (…).

Se asegurará siempre que el archivo encriptado y la clave no se facilitan en la misma comunicación".

- 8.1 Acceso a datos a través de redes de comunicaciones.
  "Todos los usuarios (tanto personal de plantilla como externos) y administradores deben identificarse y autenticarse para el acceso a sistemas y aplicaciones, tanto en red local como remotamente.

  La transmisión a terceros de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

- 8.9 Cifrado en la distribución o salida de soportes automatizados de datos.
  "(…) No se realizarán tratamientos de datos de carácter personal en dispositivos portátiles que no permitan su cifrado y siempre que el dispositivo se encuentre fuera de los locales de Accem los documentos que contengan datos de carácter personal deben de estar cifrados".

- 8.10 Copias de respaldo y de recuperación.
  "(…) Los soportes utilizados para las copias de seguridad cumplirán en su distribución las normas relativas a cifrado de los datos o mecanismo equivalente que garantice que la información no puede ser accedida o manipulada durante su transporte, o cuando se encuentren fuera de las instalaciones de Accem (…)".

  El motivo por el que solo parte de los datos de la copia de seguridad se encontraban encriptados en el momento de la desaparición del disco duro externo, es que en el Manual de Seguridad de ACCEM sólo se contemplaba la encriptación en el momento del transporte del mismo o cuando se encontrase fuera de las instalaciones de ACCEM, en las que debía estar en todo momento bajo doble llave menos cuando se estuviese realizando la copia bajo la supervisión de la responsable provincial (medida de seguridad específica de la sede recogida en el esquema de red de la misma y en el análisis de riesgos, cuya copia han aportado).
  La única parte de la copia de seguridad encriptada era la del ordenador de la responsable provincial, el cual sólo contenía parte de los datos personales del personal de la sede. Después de supervisar de forma personal la copia del contenido de los demás ordenadores en el disco duro externo, la responsable provincial realizaba la suya y tenía la costumbre de realizarla encriptada. No se consideró necesario que el resto del personal encriptase también su parte, porque el disco duro externo se guardaba bajo llave.

  En relación con la Información sobre la existencia de compromisos de confidencialidad suscritos por los empleados/as de la entidad, informan que

todos los empleados/as de la entidad firman el siguiente compromiso de confidencialidad en su contrato laboral:

"Cuarta. CONFIDENCIALIDAD: Como consecuencia de la relación laboral, el/la trabajador/a tendrá acceso y se le suministrará cierto tipo de información relativa a usuarios y servicios considerados por ambas partes como confidenciales. En consecuencia, el/la trabajador/a mantendrá bajo confidencialidad estricta, la información intercambiada, que no podrá ser objeto de revelación sin previa autorización por escrito de la Dirección de Accem, a persona alguna o forma alguna, en su totalidad o en parte, y que no será utilizada en forma distinta o contraria a los objetivos establecidos en este acuerdo.

La información confidencial no podrá, en ningún caso, ser utilizada para fines de competencia.

En esas comunicaciones están incluidos los correos electrónicos.

El presente compromiso de confidencialidad se mantendrá vigente durante la duración del contrato de trabajo en las actividades de colaboración citadas anteriormente, así como una vez que el trabajador deje de prestar sus servicios en Accem".

"Novena. La cuenta, o cuentas de email que pudieran ser asignadas al personal de Accem o aquellas a las que pudiera tener acceso durante la vigencia de su contrato son para uso exclusivamente profesional y su contenido, incluyendo emails enviados y recibidos, pertenece a la organización por lo que su contenido no se considera de uso personal y/o privado. La eliminación o manipulación de los correos electrónicos recibidos o enviados durante el periodo de prestación de servicios o con ocasión de la finalización del contrato de trabajo con fines ilícitos o con voluntad de causar un perjuicio a la Entidad, podrá dar lugar al ejercicio de acciones legales y/o disciplinarias por parte de Accem. El uso de dichas herramientas únicamente está autorizado durante la vigencia del contrato de trabajo suscrito entre las partes. El acceso y uso de las bases de datos de contactos es confidencial por lo que no podrán ser utilizados los contactos a los que se tiene acceso por cuestiones laborales para uso personal y/o privado. En caso de conflicto, bien sea dentro del equipo de trabajo o con destinatarios de correos electrónicos del personal de Accem, o cuando se detecte que no se ha realizado un buen uso del correo electrónico conforme a lo anterior, se podrá exigir al trabajador/a que remita copia de los correos enviados a las/os responsables que se estime convenientes durante un tiempo determinado. En caso de detectar una incidencia durante el uso del correo electrónico, se debe poner en conocimiento de Informática y de Calidad y Protección de Datos de manera inmediata".

"Decima. Los medios informáticos puestos a disposición del trabajador/a, son herramientas de trabajo propiedad de la empresa, tanto en relación con el hardware y con el software instalado como en relación con los contenidos, y como tales herramientas deberán ser considerados. Por ello, la empresa podrá realizar los controles que estime oportunos sobre la utilización de tales medios puestos a su disposición, a lo cual ésta expresamente autoriza, dado que los contenidos se considerarán a todos los efectos como documentación de la

empresa. El/la trabajador/a será responsable del uso de su contraseña personal, así como de la custodia de todos los documentos existentes en su ordenador, no pudiendo hacer uso de su contenido para fines distintos de los laborales, revelar o difundir su contenido ni obtener copias mediante cualquier procedimiento para utilizarlas fuera del ámbito de la empresa, salvo que tenga autorización expresa de la empresa para ello".

Adjuntan copia de los contratos laborales firmados por el personal de ACCEM de la sede de Vitoria dónde figuran las cláusulas indicadas anteriormente. En algunos casos se adjunta un anexo en vez del contrato original, debido a que los/las empleados/as más antiguos/as han firmado varias cláusulas de actualización de su contrato en febrero de 2018, entre las que se encuentran las relacionadas con la confidencialidad.

Por último, en relación con el resto de controles de seguridad asociados a la confidencialidad de la información por parte de los/las empleados/as:

- Se indica al personal que custodie los documentos bajo llave.
- Se indica al personal que bloquee el ordenador si abandona su puesto de trabajo y que no deje papeles a la vista.
- Está prohibido instalar programas de fuentes desconocidas o no autorizadas.
- Se cambia periódicamente la contraseña y con unos requisitos mínimos. El servidor solicita el cambio de forma automática.
- Cada vez que se accede a un expediente físico con datos sensibles se debe de completar el registro de acceso indicando quién accede, la fecha y firmando el mismo.
- Se indica que no se pueden abrir correos electrónicos ni archivos adjuntos de fuentes desconocidas o sospechosas.
- Se hace incidencia en el principio de minimización de datos indicando que no se deben comunicar más datos de los necesarios a compañeros/as que no deban conocerlos.
- Se recuerda el deber de secreto profesional y la prohibición de comunicar datos a personas ajenas a ACCEM.
- Si se comunican los datos de forma externa a través del correo electrónico deben encriptarse los mismos.

ACCEM ha difundido las instrucciones anteriores a los trabajadores a través de la circular interna de seguridad cuya copia aportan. Indican que la circular interna de seguridad está presente en todos los tablones de todas las sedes de ACCEM aportando fotografía del tablón de la sede de ACCEM en Vitoria dónde se puede observar la circular de seguridad. Por otro lado, la circular interna de seguridad se encuentra disponible en la carpeta de protección de datos ubicada en cada ordenador en el momento de la brecha y en el servidor en la actualidad. En la carpeta común de Protección de Datos también está disponible el Manual de Seguridad.

Se comprueba que la circular interna de seguridad se trata de un folleto explicativo fechado el 08/02/2019 que entre otras indicaciones recoge

"Recuerda mantener la información confidencial en un lugar seguro (armarios bajo llave). Mantén la mesa limpia de documentos."

Manifiestan así mismo que la responsable de seguridad de ACCEM ha dado formación a los empleados de la sede de ACCEM en Vitoria, y que en dicha formación se ha insistido en los conceptos anteriores.

Respecto a las acciones emprendidas y las medidas implementadas como consecuencia de la ocurrencia de la brecha:

Después de tratar de localizar sin éxito el disco duro externo y de preguntar a todo el personal, la responsable provincial se puso en contacto con la delegada de protección de datos para notificar la incidencia de seguridad sobre las 11 de la mañana.

La delegada de protección de datos solicitó a la responsable provincial que volviese a investigar a todo el personal para tratar de localizar el disco duro y que se comprobase que no se ha extraviado dentro de la propia sede.

La delegada de protección de datos informó sobre las 12:00 de la mañana del 22 de julio de 2019 a la Dirección de ACCEM de la brecha de seguridad y tras la reunión mantenida se ha acordado:

- Realizar un informe de la situación. El informe se ha completado con la denuncia de la Policía al día siguiente y se ha adjuntado a la declaración de la brecha de seguridad realizada a la AEPD.
- Informar a las personas cuyos datos puedan estar comprometidos de la brecha de seguridad. Se ha colgado en el tablón de anuncios de la sede de ACCEM en Vitoria una notificación cuya copia adjuntan esa misma mañana y se ha llamado por teléfono a las personas cuyos datos están comprometidos para informarlas. Aportan también foto del tablón de ACCEM dónde se puede visualizar la notificación expuesta.
- Se ha acordado que, si en el plazo de 24 horas el disco duro no aparecía, se denunciarían los hechos ante la Ertxanta para que investigase su paradero y que posteriormente se notificaría la brecha de seguridad a la AEPD.
- Se ha acordado realizar una formación de Protección de Datos en la sede de Accem en Vitoria para reforzar las medidas de seguridad y comprobar *in situ* la correcta ejecución de las mismas. Dicha formación se ha realizado por la delegada de protección de datos el día 30 de julio de 2019 (Aportan copia del registro de asistencia de los empleados a la formación).

El día 23 de julio de 2019, se vuelve a tener otra reunión entre Dirección y la delegada de protección de datos a primera hora y se revisan las medidas de seguridad, llegando a la conclusión de que es necesario tomar las siguientes medidas:

- Enviar un correo electrónico a todos los responsables territoriales y provinciales indicando que **en caso de realizarse la copia de seguridad en un dispositivo**

externo es necesario que se encripte el contenido del mismo y se guarde bajo doble llave. Se les vuelve a adjuntar a los responsables la guía para encriptar y la guía para realizar copias de seguridad. **En el correo se exige a los responsables provinciales que ese mismo día envíen una declaración jurada de que en sus sedes se han tomado estas nuevas medidas.** Aportan copia del correo remitido a todos los responsables. Indican que todos los responsables provinciales han remitido la declaración jurada solicitada.

- Modificar el Manual de Seguridad para **hacer constar que en las sedes dónde las copias de seguridad se realicen en dispositivos externos, el contenido de las mismas se debe de encriptar a pesar de que se guarde el dispositivo bajo doble llave** (Aportan copia de la nueva versión del Manual de Seguridad).

En vista de que el disco duro no se había localizado (a pesar de haberse buscado de forma intensiva) se dio orden a la responsable provincial de que realizase la denuncia de los hechos en la Ertxanta. La responsable provincial formalizó la denuncia el día 23 de julio de 2019 a las 18:45 horas. La denuncia presentada se ha adjuntado a la notificación de la brecha de seguridad realizada por la delegada de protección de datos ese mismo día a las 21:53.

Se ha esperado para notificar la brecha de seguridad a la AEPD a tener la mayor información posible de la incidencia y a haber presentado la denuncia en la Ertxanta.

En cuanto a la información sobre si se ha tenido conocimiento de la utilización posterior de los datos personales sustraídos, ACCEM no ha tenido conocimiento de que dichos datos se hayan utilizado ni de que nadie haya tenido acceso a los mismos.

Por otro lado, en cuanto a la información sobre si se han modificado los aspectos de seguridad y compromisos de confidencialidad de los empleados con posterioridad a los hechos, se ha modificado el Manual de Seguridad de ACCEM como se ha indicado anteriormente, pero no se ha visto necesario modificar los compromisos de confidencialidad de los/las empleados/as. ACCEM no sabe cómo ha podido desaparecer el disco duro externo y como se indica en el informe de la brecha de seguridad realizado, ante la perspectiva de que lo haya podido sustraer alguien, es más probable que haya podido ser alguien del personal que una persona externa a la entidad. La afirmación anterior se desprende de que ninguna persona externa accede al despacho de la responsable ni accede a las oficinas sin supervisión, pero no se tiene constancia de que ningún/a trabajador/a concreto haya sustraído el disco duro externo.

A raíz de la desaparición del disco duro externo se ha modificado el apartado 8.10 del Manual de Seguridad de ACCEM, y se ha especificado que cuando las copias de seguridad se realicen en dispositivos portátiles, los mismos deben de encriptarse también dentro de la oficina y guardarse bajo doble llave. Aportan copia de la nueva versión del Manual de Seguridad de ACCEM.

Los soportes utilizados para las copias de seguridad se conservarán bajo doble llave en lugar adecuado y cumplirán las normas relativas a cifrado de los datos o mecanismo equivalente que garantice que la información no puede ser accedida o manipulada, tanto dentro como fuera de las instalaciones de ACCEM.

Por último, en cuanto al detalle de las actuaciones policiales y resultados de las mismas que se hayan puesto en conocimiento de la entidad, ACCEM ha contactado con la Ertxanta para facilitarle el número de serie del disco duro externo sustraído al día siguiente de la formalización de la denuncia. Ante la pregunta por el avance de la investigación, la Ertxanta ha indicado que si tienen alguna novedad se pondrán en contacto directamente con ACCEM. A fecha de la contestación emitida a esta Agencia, la entidad no ha tenido ninguna novedad de la investigación ni del paradero del disco duro externo.

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 que a su vez se encontraba en un despacho con llave. Solo disponían de las llaves de acceso al despacho cierto personal arriba indicado. Sin embargo, es cierto que el soporte sustraído estaba encriptado parcialmente y solo la encriptación era completa cuando salía de la sede, según consta en los protocolos de seguridad a fecha del incidente.

En cuanto a las medidas adoptadas para minimizar el impacto del incidente, cabe señalar que se procedió a actualizar el manual de seguridad incorporando la obligación en lo sucesivo de proceder a la encriptación total del soporte de copia de seguridad y se ha instalado un servidor adicional que las realiza de forma automática, entre otras medidas arriba indicadas.

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 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.

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 ***ACCEM,*** con NIF ***G79963237*** y domicilio en ***PLAZA SANTA MARIA SOLEDAD TORRES ACOSTA, 2 PISO 3 - 28004 MADRID.***

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