- **Procedimiento Nº: E/01557/2020**

## 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 17 de febrero de 2020 la Directora de la Agencia Española de Protección de Datos (en adelante, AEPD) acuerda iniciar actuaciones de investigación en relación a una brecha de seguridad de datos personales notificada por doña ***A.A.A.*** (en adelante, delegada de protección de datos o DPD) con NIF ******NIF.1***, relativa a la sustracción de ordenador portátil a una docente con datos de alumnos/as.

**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: 13 de febrero de 2020

ENTIDADES INVESTIGADAS

Viceconsejería de Educación de la Consejería de Educación, Cultura y Deportes de la Junta de Comunidades de Castilla-La Mancha (en adelante Viceconsejería), con NIF S1911001D y domicilio en Bulevar Río Alberche S/N, 45071 Toledo.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Respecto a los hechos, la Viceconsejería, en calidad del responsable del tratamiento de datos, manifiesta lo siguiente:

- Que el 11 de febrero de 2020 a las 8:30 horas, una docente del Colegio de Educación Infantil y Primaria ******COLEGIO.1*** (en adelante, el CEIP), sito en ******LOCALIDAD.1***, estacionó su vehículo particular en la citada localidad dejando en su interior el ordenador portátil laboral de la Junta de Comunidades de Castilla-La Mancha guardado en una bolsa sin distintivo. La Viceconsejería declara que la zona de estacionamiento en cuestión está vigilada por cámaras de seguridad gestionadas por los establecimientos del entorno.
- Que la jornada escolar empieza a las 9:00 horas, lapso de media hora en que la docente es avisada de que le han roto la ventanilla del vehículo y detecta la sustracción del ordenador portátil que contenía datos con los que llevaba el seguimiento personalizado de sus alumnos/as durante el curso.
- Que inmediatamente la docente llamó por teléfono a la directora del CEIP comunicando la sustracción del ordenador portátil laboral, y que la directora le consulta sobre los posibles datos del alumnado que han podido verse involucrados, así como que le indica a la docente que proceda a denunciar los hechos ante la Guardia Civil.

- Que la directora del CEIP es informada por la docente implicada de que el ordenador portátil sustraído tiene guardadas sus claves de las siguientes aplicaciones informáticas institucionales utilizadas en el ámbito educativo de la comunidad autónoma de Castilla-La Mancha: DELPHOS (sistema de gestión para la red de centros educativos) y PAPÁS 2.0 (plataforma educativa con el objeto de facilitar la gestión administrativa a los ciudadanos en los diferentes procesos educativos convocados, conteniendo los espacios de ******ESPACIOS.1***
- Que a las 9:00 horas del mismo día la directora del CEIP realiza una llamada telefónica al área responsable de protección de datos de la Junta de Comunidades de Castilla-La Mancha para saber cómo proceder.
- Que a las 9:23 horas del citado día la docente que ha sufrido la sustracción del ordenador portátil laboral comparece ante la Guardia Civil, en el puesto principal de ******LOCALIDAD.1***, para la interposición de la correspondiente denuncia. A fecha de 5 de marzo de 2020, la Viceconsejería manifiesta desconocer las actuaciones realizadas por la Guardia Civil al respecto.
- Que el ordenador portátil sustraído había sido formateado en septiembre de 2019 y que en el momento de la sustracción no disponía de contraseña de acceso alguna. Además, la Viceconsejería manifiesta no haber podido esclarecer los datos de los alumnos que contenía dicho ordenador, aunque estima unos 50 alumnos/as implicados con:
    - Nombre y apellidos.
    - Nombre de pila de los progenitores.
    - Número de móvil de los progenitores, y de fijo si lo hubiera.
    - Calificaciones de los cursos 2017/2018 y 2018/2019.

  También, la Viceconsejería posee dudas sobre si disponía de listas de alumnos (nombres y apellidos ordenados) del CEIP en 2º y 6º curso de Educación Primaria, es decir, de 7 y 11 años, así como fotografías de actividades realizadas con los alumnos a lo largo del curso.
- Que no existe tipo de causa alguna ni condiciones puntuales que facilitasen la sustracción del ordenador portátil laboral a la docente. Igualmente, la Viceconsejería expone no tener constancia de la utilización por terceros de los citados datos personales implicados en la brecha de seguridad en cuestión.

2. Respecto a las medidas previas al acontecimiento de la brecha de seguridad, la Viceconsejería, en calidad de responsable del tratamiento, informa de lo siguiente:

- Aporta un RAT (registro de actividades de tratamiento) en el que se le puede identificar como responsable del tratamiento de los datos en la actividad de gestión del alumnado, la cual se define como gestión administrativa y educativa del alumnado de centros docentes de Castilla-La Mancha.
- La DPD (notificante de la Brecha de seguridad) señala al *Decreto 57/2012, de 23 de febrero, por el que se establece la política de seguridad de la información en la Administración de la Junta de Comunidades de Castilla-La Mancha* (Diario Oficial de Castilla-La Mancha de 28 febrero de 2012 con corrección de errores de 13 de marzo de 2012) como su fuente de política de

seguridad de la información y su marco organizativo y operacional en la gestión de datos de los ciudadanos castellanomanchegos.

- La DPD aporta un AA.RR. (análisis de riesgos) del área TIC (tecnologías de la información y de la comunicación) referido a las comunicaciones, a los sistemas, a la infraestructura CPD (centro de proceso de datos) y a la atención a usuarios de la Junta de Comunidades de Castilla-La Mancha con fecha 24 de junio de 2019. Sin embargo, no incluye AA.RR. asociado al tratamiento de datos que realiza la Viceconsejería, es decir, únicamente se valora el impacto que tendría un incidente que afecte a la seguridad de la información y los sistemas, respecto a las dimensiones de: disponibilidad, integridad, confidencialidad, autenticación y trazabilidad.
- La DPD presenta certificado de auditoría y conformidad al ENS (esquema nacional de seguridad), en el ámbito de la Administración electrónica, de los sistemas de información que soportan la prestación de servicios comunes de Tecnología de la Información y Comunicaciones de la Junta de Comunidades de Castilla-La Mancha.
- No consta haber realizado EIPD (evaluación de impacto relativa a la protección de datos) asociado a posibles riesgos alegando la DPD que:

  *"no existe constancia de que este tratamiento haya sufrido ninguna modificación sustancial que implique nuevos riesgos a los derechos y libertades de las personas ni cambios tecnológicos que aconsejen que se acometa esta medida"*.
- Señala el obligado cumplimiento de la *Orden de 11/07/2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento, por la que se aprueba la instrucción sobre el uso aceptable de medios tecnológicos en la Administración de la Junta de Comunidades de Castilla-La Mancha* (Diario Oficial de Castilla-La Mancha de 30 de agosto de 2012) por parte del personal de la Administración de la Junta de Comunidades de Castilla-La Mancha que utilice los medios electrónicos de la citada Administración, en cuyo artículo quinto concretamente se señala lo siguiente:

  *<1. Los dispositivos móviles, ya sean del centro o personales (portátiles, tabletas) en los que haya guardados datos y/o del alumnado del centro deberán estar protegidos con contraseña, huella … incluidos pendrive o discos duros portátiles.*

  *2. Se recomienda poner nombre e iniciales de los apellidos.*

  *3. Una vez finalizado el curso, dichos datos y/o fotos deberán ser eliminados de dichos dispositivos, en caso de necesitar mantener una copia, esta será guardada en el servidor del centro, quien se encargará de custodiar dichos documentos.*

  *4. No se podrán guardar por defecto las contraseñas de las plataformas Delphos y Papas.>*
- Acredita disponer de dos comunicaciones generales dirigidas a directores y secretarios de los centros educativos de su comunidad autónoma con información sobre la protección de datos de carácter personal, en las que resumen aspectos relevantes y novedosos de la normativa sobre protección de

datos de aplicación, las cuales dicen haber sido remitidas a los destinatarios por correo electrónico.

- Informa haber convocado distintos cursos dirigidos a los centros educativos sobre protección de datos de carácter personal, así como atender por su parte y por la de la DPD consultas de los centros educativos por correo electrónico.
- Expone dar la opción de proponer la creación de tratamientos de datos en el RAT correspondiente, a través de PAPÁS 2.0. Asimismo, la Viceconsejería señala la existencia de un apartado específico en el Portal de Educación de la Junta de Comunidades de Castilla-La Mancha, en el que figura diversa información y documentación de protección de datos en su ámbito:

  ******URL.1***
- Que en su plataforma corporativa PAPAS 2.0 conectada al sistema DELPHOS se recogen instrucciones para la generación de contraseñas a través de sistemas seguros y ciertas indicaciones en materia de protección de datos. La Viceconsejería aporta como evidencias un ejemplo de documento generado por la plataforma para la entrega de credenciales de acceso (usuario y clave) y copia de las capturas de pantalla de algunas indicaciones.
- Presenta los módulos de comunicación de los manuales de uso de la plataforma PAPAS 2.0 para alumnos, para coordinadores de centros educativos y para profesores, en los que extracta las consideraciones de tratamiento de datos personales referidos a cada tipo de usuario.
- La Secretaría del CEIP certifica que dicho centro educativo, en septiembre de 2019, recabó las autorizaciones para la toma y tratamiento de imágenes, según el modelo facilitado por la Junta de Comunidades de Castilla-La Mancha, las cuales se encuentran custodiadas junto a los expedientes del alumnado en dicho centro.

<u>3. Respecto a las medidas posteriores al acontecimiento de la brecha de seguridad:</u>

3.1. De carácter correctivo (reactivas tras la brecha de seguridad):

o La directora del CEIP certifica que el mismo día 11 de febrero de 2020, cuando recibe la llamada de la docente relativa a la sustracción del portátil, se le reasigna nueva clave de usuario de DELPHOS (y por ende de acceso a PAPAS 2.0), de tal forma que pierde validez la guardada en el ordenador portátil sustraído.

o La Viceconsejería declara no haber realizado comunicación a las familias del CEIP con posibles datos afectados en la brecha de seguridad porque entiende que, en principio, no existe un alto riesgo para los derechos y libertades de esas personas físicas. En este sentido, la Viceconsejería defiende cumplir con lo dispuesto en el artículo 34 del RGPD.

3.2. De carácter preventivo (proactivas para evitar que se repita la brecha de seguridad):

o El 13 de febrero de 2020, la Viceconsejería presenta dos comunicaciones (idénticas en contenido, una por medio de correo electrónico y la otra como mensaje a través de la plataforma PAPAS 2.0) de la directora del CEIP presuntamente dirigidas al profesorado integrante del claustro, con indicaciones

de seguridad a seguir respecto a los datos personales en los mismos términos del arriba citado artículo 5 de la *Orden de 11/07/2012.*

Resultando especialmente remarcable la necesidad de que los dispositivos móviles de uso laboral han de contar con la protección de una contraseña.

## 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, respecto de las contraseñas de acceso a las aplicaciones corporativas, si bien existían, se encontraban guardadas en el propio portátil sustraído, por lo que en el mismo momento en que se notificó la sustracción al CEIP se procedió a reasignar nuevas claves.

Consta también contemplado el riesgo de robo del portátil y el modo de actuación a seguir conforme a un protocolo predeterminado que se llevó a efecto, en concreto, se debe notificar al responsable al objeto de tomar las medidas preventivas para minimizar el impacto de la brecha de seguridad. Siguiendo el citado protocolo, se procedió interponer denuncia ante la Guardia civil.

No obstante, si bien no consta acreditado la existencia de datos personales -al margen de los contenidos en las aplicaciones corporativas con acceso mediante clave- y con posible acceso a terceros, se debe reforzar en su ámbito competencial el cumplimiento de lo dispuesto en la citada *Orden de 11/07/2012, de la Consejería de Presidencia y Administraciones Públicas y de la Consejería de Fomento,* que obliga, entre otras, a la encriptación de soportes digitales que contengan datos personales.

En consecuencia, acaecido el riesgo de desaparición del portátil, 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 extraíbles y copias de seguridad parece suficiente para evitar el impacto de 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 de los alumnos (nombre, iniciales de apellidos, teléfono de progenitores y notas del curso 2018/2019)

contenidos en el soporte hayan sido objeto de tratamiento posterior por terceros ajenos, ni constan reclamaciones ente la AEPD por los afectados.

**III**

Se debe señalar, que de acuerdo con el artículo 33.1 del RGPD, en caso de violación de la seguridad de los datos personales es el responsable del tratamiento quien lo notificará, en los términos oportunos, a la autoridad de control, la AEPD en este caso, y no el delegado de protección de datos. A la par, el artículo 39.1.e) del RGPD señala entre las funciones del delegado de protección de datos el actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, por lo que, presumiblemente, en esta brecha de seguridad se han malinterpretado las responsabilidades de ambas figuras (responsable y DPD) vinculadas al tratamiento de los datos de la Viceconsejería.

**IV**

Por lo tanto, se ha acreditado que la actuación tanto del CEIP como de la Viceconsejería 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:

Viceconsejería de Educación de la Consejería de Educación, Cultura y Deportes de la Junta de Comunidades de Castilla-La Mancha, con NIF S1911001D y domicilio en Bulevar Río Alberche S/N, 45071 Toledo.

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