- **Procedimiento Nº: E/12017/2019**

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 inician por la recepción de un escrito de notificación de brecha de seguridad calificada de "confidencialidad de datos personales" remitido por la VICECONSEJERÍA EDUCACIÓN DE LA JUNTA DE CASTILLA LA MANCHA en el que informa a la Agencia Española de Protección de Datos de que un alumno de un centro escolar fotografió con el teléfono móvil y subió a Instagram las papeletas de candidatos a la elección del consejo escolar en las que figuraba: nombre, apellidos y DNI de los candidatos.

SEGUNDO: La Subdirección General de Inspección de Datos inicia actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la notificación de violación de seguridad, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación inicial de la brecha de seguridad: 5 de diciembre de 2019

Fecha de notificación adicional de la brecha de seguridad: 18 de diciembre de 2019

ENTIDADES INVESTIGADAS

Viceconsejería de Educación de la Junta de Castilla-La Mancha, con NIF S1911001D y con domicilio en Avda de Portugal 11, 45071 Toledo.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 14 de enero de 2020 la Inspección de Datos remite escrito de solicitud de información a la Viceconsejería de Educación de la Junta de Castilla-La Mancha (en adelante Viceconsejería) y de la respuesta recibida con fecha 18 de febrero de 2020 ponen de manifiesto lo siguiente:

   Respecto a la cronológica de los hechos

   1.1. Con fecha 3 de diciembre de 2019, la directora de un Instituto de Educación Secundaria en Toledo, remite correo electrónico a la unidad dependiente de la Secretaría General de la Consejería de Educación, Cultura y Deportes, encargada del asesoramiento interno a los servicios responsables de la Viceconsejería en las materias de calidad y simplificación administrativa, transparencia y protección de datos. Los hechos que la Directora del centro educativo relata en ese correo son los siguientes:

"El miércoles pasado, 27 de noviembre jornada de elecciones al Consejo Escolar de centro, tuvimos un caso de difusión de datos el cual le trasladé a nuestra inspectora ... el mismo día vía mail y personalmente el viernes 29. Le explico el hecho: La Jefa de Estudios y los dos representantes de alumnos de la mesa de dicho sector pasaban por todas las clases con las papeletas y en cada clase se iba comprobando el censo y los alumnos iban votando. A 4a hora, una de las alumnas candidatas me enseñó una captura de pantalla de Instagram en la que figuraba la papeleta de las votaciones del consejo con el nombre de los 5 chicos y su DNI, papeleta generada así por Delphos. Un chico de 1º de uno de nuestros ciclos de Grado Medio, que tiene 20 años y problemas disciplinarios varios, le había hecho una foto a la papeleta cuando llegó el turno de votación a su aula y la había compartido con más de 250 personas. El hermano de esta chica le reenvió los DNIs tachados y nuestro alumno contestó subiendo una nueva foto de la papeleta diciendo que la culpa era del centro. Tenemos las dos capturas del móvil archivadas, por si fuera de su interés. Entendemos que debemos sancionar al alumno según nuestras NCOF por uso del móvil en horario escolar, pero nuestra duda es si cabe denuncia externa al respecto".

El mismo día de recepción del mensaje, la unidad de protección de datos de la Consejería de Educación, Cultura y Deportes (en adelante Consejería), remitió un correo electrónico a la Directora del centro docente, con copia a la Delegada de Protección de Datos de esa Administración y a la Jefa de Servicio dependiente de la Viceconsejería encargada de la gestión del proceso de elecciones del Consejo Escolar, recordando al centro docente el procedimiento existente para la notificación de brechas de seguridad. Así mismo, se solicita al Centro la documentación acreditativa del incidente.

1.2. Con fecha 4 de diciembre de 2019, la Directora del centro, atendiendo a la solicitud efectuada por la unidad de protección de datos, remite a la Consejería copia de la papeleta del sector alumnos del Consejo que fue difundida indebidamente, así como de las dos capturas de pantalla que reflejan el incidente y del correo electrónico remitido el mismo día del incidente a la Inspección de Educación.

El mismo día (4-12-2019) la unidad de protección de datos de la Consejería envía un segundo correo electrónico a la Delegada de Protección de Datos y al Servicio de Seguridad y Protección de Datos dependiente de la Dirección General de Administración Digital de la Consejería de Hacienda y Administraciones Públicas, órgano competente en esta materia conforme a lo establecido en el artículo 12.2 del Decreto 80/2019, de 16 de julio, por el que se establece la estructura orgánica y competencias de la Consejería de Hacienda y Administraciones Públicas (D.O.C.M. nº 141, de 18 de julio de 2019), acompañados de la documentación obtenida.

Tal y como consta en dicha comunicación, la unidad informa de que, a la vista de la revisión del incidente y del relato de los hechos efectuados por el centro docente que comunicó la incidencia, se advierte un error en el sistema informático de gestión para red de centros educativos de la Comunidad Autónoma en la elaboración de las papeletas del proceso electoral de los Consejos Escolares, ya que en las Instrucciones de 2-10-2019 dictadas por la Viceconsejería de Educación para la gestión del proceso electoral, se ordena expresamente

que en las papeletas se recoja exclusivamente los nombres y apellidos, y no los DNI, de los candidatos electorales (Instrucción vigesimoquinta) y, sin embargo, tal y como expone el centro docente, dicha aplicación informática genera automáticamente las papeletas incluyendo también ese último dato personal DNI).

El mismo día (4-12-2019), el Servicio de Seguridad y Protección de Datos solicita a la Consejería que se ponga en contacto con el centro docente para que solicite a Instagram la retirada del contenido difundido indebidamente, indicando para ello el enlace disponible en la página web de esa Agencia Española de Protección de Datos con información para poder eliminar contenido subido a las redes sociales sin el consentimiento de las personas afectadas:

Atendiendo a esta solicitud, en la misma fecha (4-12-2019), la unidad de protección de datos de la Consejería solicita mediante correo electrónico dirigido al centro docente afectado la aplicación de esta medida cautelar

1.3. Mediante correo electrónico remitido el día 5-12-2019, la Jefa de estudios del centro docente afectado comunica a la unidad de protección de datos que en la tarde del día anterior solicitaron la retirada de las imágenes de la papeleta de voto, identificando la cuenta de Instagram del alumno que difundió la información así como el enlace de su perfil. Este correo se reenvía por la unidad de protección de datos en la misma fecha a la Delegada de Protección de Datos.

1.4. Con fecha 5-12-2019, la Delegada de Protección de Datos remite correo electrónico a la unidad de protección de datos de la Consejería informando que ya se ha notificado el incidente a la Autoridad de Control (AEPD).

Así mismo la Delegada de Protección de Datos recomienda a la Viceconsejería de Educación, órgano responsable del tratamiento de datos en el que se produjo el incidente, las dos actuaciones siguientes:

- Dirigir una comunicación interna de trabajo al personal informático encargado del desarrollo y mantenimiento de las aplicaciones y sistemas informáticos, dependiente de la Dirección General de Administración Digital de la Consejería de Hacienda y Administraciones Públicas, solicitando la modificación del programa de gestión de la red de centros docentes "Delphos", para que no figuren los DNI en las papeletas que se generen en próximas convocatorias electorales.
- Que se recomiende a los centros la destrucción de las papeletas electorales del proceso electoral ya finalizado.

Por último, la Delegada de Protección de Datos comunica a la Consejería que, una vez disponga de las evidencias que demuestren la implantación de las acciones recomendadas, o aquellas que se consideren más oportunas por el órgano responsable del tratamiento, se lo comuniquen para proceder al cierre de la brecha de seguridad.

1.1. Ambas medidas recomendadas por la Delegada de Protección de Datos (DPD) fueron atendidas por la Viceconsejería:

- Con fecha 9-12-2019 la jefa del Servicio encargado de la gestión de las elecciones del Consejo Escolar remitió un correo electrónico a la uni-

dad de la Dirección General de Administración Digital responsable del desarrollo y mantenimiento del sistema Delphos comunicando la brecha de seguridad detectada en el proceso de elección a Consejos Escolares y solicitando la corrección del proceso de emisión automática de las papeletas en las próximas elecciones de los Consejos escolares a celebrar el año que viene, para que se evite que figuren los DNI de las personas que constan en las papeletas para votar, tal y como se ordenaba ya, por otra parte, en las instrucciones emitidas por la Viceconsejería de Educación en este último proceso electoral, Instrucciones que, según indica la propia jefa de servicio, fueron *"remitidas a Delphos y a todos los centros educativos de la Región"*.

- Con fecha 13-12-2019 la Viceconsejería remitió una comunicación a todas las Delegaciones Provinciales de la Consejería, con la siguiente indicación: *"Una vez celebradas las votaciones para la elección y renovación de los Consejos Escolares de los centros docentes sostenidos con fondos públicos que imparten enseñanzas no universitarias en Castilla-La Mancha, desde esta Viceconsejería se solicita que os dirijáis a los centros de vuestra provincia en los que se hayan celebrado elecciones, informándoles de que por razones de protección de datos, deben proceder a la destrucción de toda la documentación del proceso con datos personales que ya no sea necesario conservar".* Se adjunta dicho correo electrónico, cuya copia fue remitida a la DPD en la misma fecha.

Respecto a las causas que han hecho posible la incidencia

1.1. De forma directa, la acción de difusión indebida en una red social ha sido realizada por una acción del alumno del centro mencionado. De acuerdo con el relato del centro educativo, a pesar de que este alumno es censurado por otra persona que le envía la papeleta con los DNI tachados, el alumno publica de nuevo la papeleta en Instagram con el siguiente comentario: *"XD. Os quejáis de que haya subido los DNI. Cuando la culpa es del centro por dar el DNI a personas ajenas xd"*.

Indirectamente, la difusión indebida del dato del DNI ha podido tener lugar también porque las papeletas generadas automáticamente en el sistema informático de gestión de la red de centros docentes han incluido por error este dato de los candidatos, junto con su nombre y apellidos.

Respecto a la tipología de datos y número de afectados

1.2. Número de personas afectadas por la incidencia: 5

Tipología de los datos afectados: datos identificativos (apellidos, nombre y DNI) de cinco alumnos menores de edad que concurren como candidatos en el proceso de elecciones al Consejo Escolar del centro durante el curso 2019/2020.

Respecto a las acciones tomadas con objeto de minimizar los efectos adversos y resolución final de la incidencia

- Solicitud a Instagram (mediante el formulario habilitado al efecto por la AEPD) la retirada de las imágenes de las papeletas electorales en las que figuran los datos identificativos de los cinco alumnos afectados.

- Comunicación del incidente a las familias de los cinco alumnos menores de edad cuyos datos se han publicado indebidamente efectuada por la Dirección del centro docente IES en ******LOCALIDAD.1***. De acuerdo con la información facilitada por la Directora del centro, la comunicación del incidente se efectuó poco después del incidente mediante llamada telefónica a cada familia.
- Solicitud de la jefa de servicio encargada de la gestión del proceso de elecciones al Consejo Escolar, dirigida al personal responsable del desarrollo y mantenimiento de los sistemas de información, dependiente de la Dirección General de Administración Digital de la Consejería de Hacienda y Administraciones Públicas, para que se subsane en próximas convocatorias de elecciones del Consejo Escolar el error informático detectado en el sistema de gestión de la red de centros docentes (Delphos) en la generación de las papeletas electorales (eliminación del DNI), mediante correo electrónico enviado con fecha 9-12-2019 a las 10:37 horas.
- Comunicación dirigida por esta Viceconsejería de Educación a las Delegaciones Provinciales de la Consejería Educación, Cultura y Deportes, para su difusión en todos los centros docentes, ordenando la destrucción de toda la documentación del proceso electoral en la que figuren datos personales, mediante correo electrónico remitido en fecha 13-12-2019 a las 10:04 horas.

Respecto a la utilización por terceros de los datos personales obtenidos

No consta que la información difundida indebidamente por un alumno haya sido utilizada por terceras personas ajenas. Según informó el centro docente en la comunicación del incidente, la información personal había sido compartida por el alumno en Instagram con aproximadamente 250 personas.

Respecto de la notificación realizada a los afectados.

El incidente de seguridad fue comunicado verbalmente, mediante comunicación telefónica, a las familias de los cinco alumnos afectados.

Respecto de la seguridad de los tratamientos afectados con anterioridad a la incidencia de seguridad:

- Aportan copia del contenido de la base de datos utilizada para la gestión del Registro de Actividades de Tratamiento referente al tratamiento Elecciones Consejo Escolar de los centros docentes.
- De acuerdo con la información facilitada por la DPD y la Dirección General de Administración Digital de la Consejería de Hacienda y Administraciones Públicas, existe un análisis de riesgos de seguridad realizado por el Servicio de Seguridad y Protección de Datos de la Consejería de Hacienda y Administraciones Públicas, código: ******CÓDIGO.1*** de fecha 24 de junio de 2019, cuyo alcance es *"Los sistemas de información que soportan la prestación de servicios comunes de Tecnología de [a Información y las Comunicaciones (TIC) a la Administración regional y al ciudadano, en infraestructura software y gestión de contenidos, infraestructura CPD, comunicaciones y atención de usuarios y puesto de trabajo, así como los activos en los que se soportan, de acuerdo con la categorización del sistema vigente".*

Este análisis de riesgos forma parte del sistema de gestión de seguridad de la información certificado de Conformidad con el Esquema Nacional de Seguridad, con vigencia hasta el 2 de agosto de 2020.

- Respecto a la Evaluación de Impacto relativa a la protección de datos, no se ha realizado puesto que este tratamiento no ha 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.

- La política de seguridad en la Junta de Comunidades de Castilla-La Mancha está recogida en el Decreto 57/2012, de 23 de febrero de 2012, por la que se establece la política de seguridad de la información en la Administración de la Junta de Comunidades de Castilla-La Mancha.

- Esta política se complementa, en cumplimiento de la medida *"Normativa de seguridad [org. 2]"* del anexo ll del Real Decreto 3/2010, de 8 de enero de 2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, con 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.

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 brecha 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, se produjo una brecha de seguridad de datos personales categorizada como brecha de confidencialidad, como consecuencia de la difusión indebida por un alumno de un centro escolar que fotografió con su teléfono móvil y subió a Instagram las papeletas de candidatos a la elección del Consejo Escolar en las que figuraba : nombre, apellidos y DNI.

Cabe señalar también, que el tratamiento del dato personal "DNI" de los candidatos que figuraba en la papeleta de votación al Consejo Escolar ya estaba prohibido por la propia normativa interna de la Consejería de Educación.

En consecuencia, nos encontramos ante dos tratamientos de datos indebidos y sucesivos.

No obstante, de las actuaciones de investigación se desprende que tanto el centro educativo como la Viceconsejería de Educación, disponían de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo que, sin embargo, no fueron las suficientes y deberán ser objeto de revisión.

Sin embargo, consta que tanto el centro educativo como la Viceconsejería de Educación disponían de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad así como la diligente reacción ante la misma al objeto de notificar, comunicar a los padres de los interesados, minimizar el impacto e implementar nuevas medidas correctoras y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de los afectados.

Por último, se recomienda elaborar un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

Por lo tanto, se ha acreditado que tanto la actuación de la Viceconsejería de Educación como el centro docente han actuado diligentemente para la resolución de la Brecha notificada y 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 al Viceconsejería de Educación de la Junta de Castilla La Mancha, con NIF S1911001D y con domicilio en Avda. de Portugal 11, 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