- **Procedimiento Nº: E/07215/2019**

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 de datos personales (en adelante brecha de seguridad) remitido por la CONSEJERÍA EDUCACIÓN Y CULTURA DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS (en adelante Consejería) en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) que una organización sindical comunicó a una funcionaria de la Consejería el resultado provisional de la fase de concurso del procedimiento selectivo para el ingreso en el cuerpo de maestros y su posterior difusión con nombres, apellidos, fecha de nacimiento, eventual concurrencia por el turno de discapacidad y DNI completo de los aspirantes, así como la puntuación provisional obtenida.

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 brecha de seguridad: 18 de julio de 2019.

ENTIDADES INVESTIGADAS

CONSEJERÍA EDUCACIÓN Y CULTURA DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS, con NIF S3333001J y con domicilio en Plaza de España 5, 33007 Oviedo, Asturias.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 6 de septiembre de 2019, la Inspección de Datos remite escrito de solicitud de información a la Consejería, reiterada el día 13 de noviembre al no recibir respuesta al anterior requerimiento.
2. De la respuesta recibida con fecha 4 de diciembre de 2019 ponen de manifiesto lo siguiente:
   - Aportan copia de un escrito de la Directora General de Personal Docente de la Consejería De Educación y Cultura del Gobierno del Principado De Asturias, sobre la fuga de información relativa al procedimiento selectivo de acceso al Cuerpo de Maestros y Maestras de la administración del Principado de Asturias, en el que se pone de manifiesto lo siguiente:
     - Primero. - A través de sendas Resoluciones de 14 de febrero de 2019 (BOPA de 18/02/2019), la Consejería con competencias en materia de Educación convoca procedimientos selectivos para el ingreso en el cuerpo de Maestros al que se refiere la Ley Orgánica 2/2006, de 3 de

mayo, de Educación, así como el procedimiento selectivo para ingreso en el Cuerpo de Maestros para personas con discapacidad intelectual, publicadas.

- Segundo. - Tal y como establece la base séptima de las bases de la convocatoria establecidas en dichas resoluciones, el sistema de selección constará de fase de oposición, fase de concurso y fase de prácticas, conforme a lo establecido en la disposición adicional duodécima de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y en el título III del Reglamento de ingreso, accesos y adquisición de nuevas especialidades en los cuerpos de funcionarios docentes a los que se refiere la Ley Orgánica 2/2006, de 3 de mayo, de Educación.
- Tercero. - En relación con la fase de concurso, la base octava de las Resoluciones citadas establece las bases correspondientes a la valoración de la fase de concurso. De acuerdo con las mismas, el 22 de junio de 2019 se procede a la publicación de la puntuación obtenida en la valoración de la fase de concurso de las personas admitidas a los procedimientos, a través del portal <***URL.1*>. Para la consulta, se estableció internamente un sistema que permitía el acceso a la valoración de forma personal, a través de la introducción del DNI y de la fecha de fecha de nacimiento de la persona interesada.
- Cuarto. - El 15 de julio de 2019, esa Consejería es alertada, a través de una funcionaria que acometía funciones de organización en el desarrollo del procedimiento selectivo, de que se encuentra disponible a través de redes sociales el listado completo correspondiente a la valoración provisional de la fase de concurso incluyendo nombre, apellidos, concurrencia por el turno de discapacidad, DNI, fecha de nacimiento y puntuación provisional obtenida en dicha fase.
- Quinto. - Dado que dicho documento no había sido publicado por esta Consejería, y únicamente era de uso interno del personal que se encargaba de la informatización del procedimiento, la Consejería registró en la herramienta de gestión de peticiones de la Administración del Principado de Asturias (APA), incidencia indicando que "*El Portal de consultas genéricas debe tener un fallo de seguridad porque anda circulando un pdf por internet con todos los datos de la tabla BBDD"*, a través de una de las personas que se encargaban de la informatización del procedimiento selectivo, y desde ******URL.1*** y el CGSI se acometen las acciones que se estiman necesarias para evitar nuevas filtraciones.

- Aportan copia del informe elaborado en relación con la fuga de información en el que se pone de manifiesto lo siguiente:
  - A las 18:26 horas del 15/07/2019 se registra en la herramienta de gestión de peticiones de la APA una incidencia indicando que *“el portal de consultas genéricas debe tener un fallo de seguridad porque anda circulando un “pdf” por internet con todos los datos de la tabla de BBDD*”. La solicitud es generada por el responsable técnico del activo tecnológico afectado (Portal de ******PORTAL.1***) por parte de la Consejería de Educación y Cultura del Gobierno del Principado de Asturias.

En la mañana del 16/07/2019, diversos medios de comunicación publican noticias alertando del "hackeo" de datos personales de los aspirantes que se presentaron al proceso selectivo del cuerpo de maestros de la Consejería de Educación y Cultura del Gobierno del Principado de Asturias.

Identificación de las causas que originaron la fuga:

- El análisis derivado del registro de la incidencia determina que la funcionalidad de búsqueda del Portal de ******PORTAL.1*** presenta un fallo de seguridad asociado a la versión del propio producto utilizado en materia de gestión de contenidos cuyo desencadenante se detalla a continuación:

Los aspirantes a las oposiciones disponen de un mecanismo de consulta que, mediante la introducción del DNI del usuario y la fecha de nacimiento, les ofrece la información relacionada con su baremación provisional personal. Una vez facilitados dichos datos, el sistema muestra la puntuación no definitiva.

El fallo presentado por la plataforma de gestión de contenidos en la versión utilizada permite que la modificación de algún parámetro en la URL mostrada en la página de resultados y presionando la tecla *Intro*, el sistema devuelve como resultado no sólo los datos del usuario que ha incorporado el DNI y la fecha de nacimiento, sino la información de todos los aspirantes al proceso (nombre y apellidos, DNI, fecha de nacimiento y baremación provisional, entre otros).

La información resultante acumulada fue exportada a un fichero PDF que, posteriormente, se distribuye por medios ajenos al propio Portal de ******PORTAL.1***

- La vulnerabilidad identificada en el comportamiento de la funcionalidad de búsqueda atiende a un agujero de seguridad denominado *"URL manipulation"* que consiste en la modificación de los parámetros que se envían al servidor web como puntos de entrada de una aplicación (Parameter Tampering), ya sea los que viajan en los formularios o en la propia URL de navegación.

Acciones tomadas con objeto de minimizar los efectos adversos

- Desde la Consejería se deshabilita el acceso a la funcionalidad de consulta de baremación temporal con carácter inmediato a la identificación del incidente de seguridad.

- El equipo de mantenimiento de la APA, responsable de los desarrollos del Portal de ******PORTAL.1***, elabora una nueva versión de las funcionalidades afectadas para su posterior despliegue en el entorno de Integración y Producción. El 16/07/2019 a las 10:23 horas de corrige la incidencia y es aplicada por parte del equipo de Gestión de Aplicaciones.

Desencadenante del ataque

- Desde el momento en que se identifica la brecha de seguridad, y en paralelo a las acciones de corrección de la incidencia, se establecen los mecanismos de búsqueda tanto a nivel de servidor de aplicaciones como sobre la infraestructura de *firewall* por la que se cursan los flujos de navegación de las peticiones realizadas a la funcionalidad afectada.

- Tras la investigación realizada se determina que el origen de la petición que realiza la descarga del fichero PDF (y que, por tanto, explota la

vulnerabilidad "Parameter Tampering") se corresponde con un usuario consumidor de los servicios de Internet ofrecidos por el proveedor Vodafone, desde la dirección IP ***IP.1**

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

- La Administración del Principado de Asturias está inmersa en un proyecto de actualización de plataformas a las últimas versiones de productos atendiendo a la aplicación de medidas de seguridad determinadas por el Esquema Nacional de Seguridad.

- La obtención de la certificación de conformidad con el ENS para un sistema de categoría MEDIA pone de manifiesto que la Organización está inmersa en un proyecto de transformación digital y la transición tecnológica a las últimas versiones de las plataformas de gestión de contenidos que está previsto finalizar en el año 2020.

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 artículo 45.1.b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), dispone lo siguiente:

<Artículo 45. Publicación.
1. Los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente. En todo caso, los actos administrativos serán objeto de publicación, surtiendo ésta los efectos de la notificación, en los siguientes casos:
(…)
b) Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el medio donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos>.

La Base 4.1 de la Resolución del 14/02/2019, por la que se regula el proceso selectivo ajustado a concurrencia competitiva, dispone lo siguiente:

< 4. Admisión y exclusión de aspirantes
4.1. Lista provisional de personas admitidas y excluidas. Finalizado el plazo de presentación de solicitudes, la persona titular de la Consejería competente en materia

de Educación dictará resolución aprobando la lista provisional de personas admitidas y excluidas. Se publicará reseña en el Boletín Oficial del Principado de Asturias, en la que se indicarán los lugares en que se encuentren expuestas al público estas listas completas. Dichas listas se expondrán en el portal educativo: ******URL.1***

Tanto los listados provisionales como los definitivos de personas admitidas y excluidas incluirán los datos, en los términos expuestos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de datos personales, turno de ingreso, obligación de acreditar el conocimiento de castellano mediante la realización de la prueba a la que se alude en el apartado 7.1 de esta convocatoria y, en el supuesto de exclusión, indicación de la causa.

Con la publicación de la resolución que declare aprobada la lista de personas admitidas y excluidas se considerará hecha la notificación correspondiente a quien sea parte interesada, a los efectos de lo que dispone el artículo 68 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.>

La Base 9.4 de la citada Resolución, dispone lo siguiente:

<9.4. Relación de aspirantes que han superado las fases de oposición y concurso.

Los tribunales publicarán en su sede la relación de aspirantes que han superado las fases de oposición y concurso remitiendo copia de la misma al órgano convocante, el cual determinará las personas seleccionadas para ser nombradas funcionarios o funcionarias en prácticas.

El órgano convocante publicará en el portal educativo www.educastur.es la relación de personas que en cada tribunal resulten seleccionadas para pasar a la fase de prácticas, remitiendo copia a cada uno de los tribunales para la publicación en la sede de los mismos.

El resto de la documentación correspondiente al desarrollo del concurso-oposición, quedará custodiado en la Consejería competente en materia de Educación.

En el supuesto de que existan aspirantes con discapacidad que hubieran participado a través del porcentaje reservado a las personas con discapacidad para el ingreso libre y hayan superado la totalidad de los ejercicios y pruebas, pero no hayan obtenido plaza de las del porcentaje de reserva, cuando su puntuación fuera superior a la obtenida por otras personas aspirantes del ingreso libre, serán incluidos por su orden de puntuación entre las opositoras y opositores de este acceso>.

Por su parte, la D.A. 1º de la LOPDGDD, dispone lo siguiente:

< Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad>.

Y la D.A. 7ª de la LOPDGDD, dispone lo siguiente:

< Disposición adicional séptima. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.
Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.>

Por último, el art 53.2.b) de la citada LPACAP, dispone lo siguiente:

<2. Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:
(…)
b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario>.

III

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 notifica una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso indebido al portal <***URL.1*** > de la Consejería de Educación y Cultura del Gobierno del Principado de Asturias, en la que se ofrecían los resultados de las calificaciones y datos personales de los aspirantes sin anonimizar los DNI de los interesados en un proceso selectivo de concurrencia competitiva.

De la normativa arriba transcrita, la publicación de los listados de aprobados en los procesos selectivos de concurrencia competitiva se atiene a lo dispuesto en las bases de la Resolución de la convocatoria (art 45.1.b), LPACAP). En este caso, la convocatoria señala /base 4.1) que el listado de aprobados en cada fase selectiva se publicará reseña en el Boletín Oficial del Principado de Asturias, en la que se indicarán los lugares en que se encuentren expuestas al público estas listas completas y que dichas listas se expondrán en el portal educativo: <***URL.1*** > (base 9.4). Añade la convocatoria que tanto los listados provisionales como los definitivos de personas admitidas y excluidas incluirán los datos, en los términos expuestos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de datos personales.

En consecuencia, en el presente caso la publicación de los listados de aprobados es preceptiva tanto en formato papel en el lugar indicado en la reseña del BOPA, como en el portal <***URL.1*** >, y siempre con la única finalidad de informar a los interesados de sus calificaciones.

Sin embargo, debido a una disfuncionalidad en el comportamiento del portal <***URL.1***>, se podía acceder a la totalidad del listado publicado, que si bien esto no conculca la norma al encontrarse el listado completo publicado en formato papel en el lugar reseñado en el BOPA, si lo hace el tratamiento posterior con distinta finalidad al difundirse por un tercero en redes sociales.

No obstante, al margen del tratamiento posterior por un tercero que si resulta contrario al principio de finalidad dispuesto en el artículo 5.1.b) del RGPD, se debe señalar que la Consejería debió extremar la diligencia en lo dispuesto en la D.A. 7ª de la LOPDGDD al no ocultar cuatro de las posiciones del DNI de los aspirantes al Cuerpo de Maestros, por lo que deberá corregir tal anomalía en la actual adaptación al ENS del sistema de información del que es responsable que está llevando a cabo, así como evitar que un futuro se repita la incidencia notificada.

También deberá incluir una nota informativa tanto en los listados en formato papel y electrónico advirtiendo que los listados de aprobados en un proceso selectivo ajustado a concurrencia competitiva que se publican y que contienen datos de carácter personal, su única finalidad, de conformidad con lo previsto en la LPACAP, es la de

proceder a notificar a cada uno de los aspirantes el contenido del procedimiento selectivo. Estos listados no podrán ser reproducidos ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de información, conforme al principio de finalidad dispuesto en el art 5 del RGPD.

No obstante, también consta que la Consejería de Educación y Cultura del Gobierno del Principado de Asturias, a través del servicio de mantenimiento de Informática de la APA, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales, así como la diligente reacción ante la misma al objeto de minimizar el impacto e implementar las medias correctoras oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento y delegado de Protección de Datos.

También debe valorase la adopción de medidas técnicas y de gestión y adecuación al ENS de todos los sistemas de información de la APA, al objeto de comprobar y, en su caso, mejorar la calidad de las aplicaciones de gestión de datos personales.

No consta en esta AEPD reclamaciones relacionadas con la brecha de seguridad notificada.

El informe final que se deberá elaborar tras el seguimiento y cierre de 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 de una brecha similar.

IV

En cuanto al tratamiento posterior por tercera persona consistente en el acceso individual a las calificaciones de los aspirantes a través de una vulnerabilidad en el sistema de acceso del portal <***URL.1*** >, tratamiento contrario al principio de finalidad expuesto en el artículo 5.1.b) del RGPD, su acumulación en un fichero en formato PDF y su posterior difusión en redes sociales a través de la dirección IP aportada desde la que se ha difundido el listado de calificaciones, no ha sido posible determinar al responsable concreto.

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.

V

Por lo tanto, se ha acreditado que la actuación de la Consejería de Educación del Gobierno del Principado de Asturias, como entidad responsable del tratamiento ha sido razonable y 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 CONSEJERÍA EDUCACIÓN Y CULTURA DEL GOBIERNO DEL PRINCIPADO DE ASTURIAS, con NIF S3333001J y con domicilio en Plaza de España 5, 33007 Oviedo, Asturias.

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