Expediente N.º: EXP202203557

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: En fecha 21 de febrero de 2022, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S0611011, recibido en fecha 7 de diciembre de 2021, en el que informaba a la Agencia Española de Protección de Datos de lo siguiente:

En fecha 2 de diciembre de 2021, se tiene conocimiento de una brecha de seguridad provocada por un ciber incidente que afectó a la confidencialidad de datos personales de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, en algunos casos con credenciales de acceso. Asimismo, tienen conocimiento de la venta de datos que tiene que ver con aplicativos e información gestionada desde el Servicio de Tecnologías de la Educación.

(…).

Aportan una IP desde donde se ha producido el ataque.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Evaluación preliminar de la notificación de la brecha de datos personales en relación con los datos aportados por el responsable y otros aspectos relevantes detectados:

1. La brecha se inicia, de forma aproximada, el 29 de noviembre de 2021. Se tuvo constancia de esta el 02 de diciembre de 2021 y se notifica ante esta Agencia el 7 de diciembre de 2021.
2. ***(…)***.
3. Los datos afectados son: datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto. NIF, Apellidos, Nombre, Teléfono, Dirección Postal, Email, Sexo, Jubilado, Discapacidad (datos parciales). Contraseñas de 18 cuentas institucionales de Educarex (el portal educativo de la Junta de

Extremadura) y contraseñas ***(…)*** de usuarios de gestión de la aplicación (no se especifica el número).
4. Volumen de 60000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma.
5. La comunicación a los afectados pendiente de decidir.
6. Indican la existencia de investigación en curso y que informarán a las autoridades oportunas.

No existen antecedentes de este mismo responsable de tratamiento relacionados con incidentes de seguridad en los sistemas de información.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA con NIF S0611001I con domicilio en AV. VALHONDO, NUM 1 - 06800 MÉRIDA (BADAJOZ)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

En fecha 18 de mayo de 2022 se decide realizar requerimiento de información al responsable de tratamiento en consonancia con la siguiente línea de investigación:

- Conocer la posible utilización por terceros de los datos personales obtenidos por la brecha.
- Conocer el estado de la posible comunicación del incidente a los afectados.
- Conocer el análisis de riesgos realizado y las medidas de seguridad preventivas y reactivas.
- Conocer el resultado de la última auditoría (obligatoria) conforme con el Esquema Nacional de Seguridad (ENS), de obligado cumplimiento por las Administraciones Públicas.
- Conocer el registro de incidentes actualizado.
- En la notificación de la brecha se indicaba que, entre los datos afectados, se encontraban datos parciales sobre discapacidad de las personas, se solicita en este punto aclaración sobre qué tipo de información se almacenaba en la base de datos filtrada.

Con fecha 1 de junio de 2022 se recibe respuesta al requerimiento anterior, de esta respuesta se concluye:

1. Afirman que no se tiene conocimiento de la utilización por terceros de los datos que pudieran haberse obtenido a través de la brecha.
2. Afirman que han analizado el riesgo causado por la brecha para los derechos y libertades de los afectados, utilizando para ello herramientas y aplicaciones propias de la Administración de la Comunidad Autónoma de Extremadura. Concluyendo lo siguiente: ***"(…)"***. Aportando también las siguientes afirmaciones:

(…).

3.Afirman que para las actividades de tratamiento de datos personales afectadas por la brecha, NO se ha llevado a cabo un proceso previo y reglado de Análisis de Riesgos, justificando para ello textualmente lo siguiente: "***(…).***"

4.Con respecto a las medidas de seguridad implementadas previamente a la brecha nos confirman las siguientes:

(…).

(…).

5.***(…).***

6.Con respecto a las medidas reactivas adoptadas tras el incidente, afirman las siguientes:

(…).

7.En relación con la copia del informe solicitado de la última auditoría conforme al ENS, afirman que NO se ha llevado a cabo un proceso de auditoría para el sistema de información indicado.

8.En relación con la aclaración de los datos de discapacidad filtrados en la brecha, contestan indicando que la base de datos únicamente almacenaba "A" o "B", por lo que se trata de una información codificada y que no se había filtrado.

Con respecto a la afirmación planteada en la respuesta del apartado 2 anterior, en el transcurso de esta investigación el inspector decide hacer uso de la herramienta COMUNICA-BRECHA RGPD con los datos que se nos ha proporcionado en la notificación de la brecha y el resultado es el siguiente: "DEBERÍA COMUNICAR LA BRECHA DE SEGURIDAD A LOS AFECTADOS". En concreto, la información utilizada como entrada en esta herramienta ha sido:

- Incidente intencionado, externo y consecuente de un ciber incidente.
- Personas u organizaciones no autorizadas han podido acceder y extraer datos.
- Los datos no estaban cifrados.
- Las personas afectadas pueden encontrar inconvenientes importantes, produciendo daño limitado, que podrán superar a pesar de algunas dificultades.
- No se tiene constancia de la materialización de alguno de los daños identificados.
- La probabilidad de materialización es baja.
- Los datos son (básicos, documento identificativo, de contacto, credenciales de acceso.
- No hay menores entre los afectados y se desconoce la existencia de colectivos vulnerables.
- La brecha afecta a unos 60000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma y se detecta el 2 de diciembre de 2021, siendo la fecha de inicio aproximada el 29 de noviembre de 2021.

Con respecto a la afirmación planteada en la respuesta del apartado 3 anterior, en la que afirman que NO disponen de Análisis de Riesgos para las actividades de tratamientos afectados por la brecha (y aportan justificación para ello), hay que hacer referencia a lo indicado en la propia política interna ***(…)*** en su apartado 7.2:

(…).

Por lo que queda constatado que, incluso según la propia Política interna de Privacidad, este análisis sí se debería haber llevado a cabo.

En relación con las medidas de seguridad implementadas previamente a la brecha, según recoge el apartado 9 de la ***(…):***

También con respecto al ENS, y en relación con la respuesta al requerimiento aportada en el apartado 7 anterior, en la que confirman que NO se ha llevado a cabo un proceso de auditoría conforme a las previsiones del Esquema Nacional de Seguridad para el sistema de información afectado por la brecha, hay que hacer referencia a lo indicado en el artículo 34 del RD 3/2010 por el que se regulaba el ENS en el momento de producirse la brecha (derogado recientemente por el Real Decreto 311/2022, de 3 de mayo de 2022), en el que se especificaba que esta auditoría era obligatoria al menos cada dos años, verificando así el cumplimiento de los requerimientos de dicho Esquema. La actual regulación del ENS (RD 311/2022) también especifica esta obligatoriedad en su artículo 31. En concreto, según marca el ENS, el objeto de esta auditoría debe abarcar los siguientes puntos (entre otros):

- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el Anexo II (Medidas de Seguridad), en función de las condiciones de aplicación de cada caso.

(…).

Este tipo de ataques son bien conocidos e identificables en las auditorías de seguridad.

Por último, con respecto a la fecha de notificación de la brecha ante esta Agencia, y según la información que se extrae del informe del incidente de seguridad (adjuntado en la contestación a nuestro requerimiento), queda constatado que:

- La brecha se detecta el día 2 de diciembre de 2021, jueves, en torno a las 18:51 horas. Es en este momento cuando se tiene conocimiento de la filtración de datos personales. Los datos estaban a la venta en un foro de internet con pago en bitcoins.
- El día 3 de diciembre de 2021, viernes, se termina de elaborar el informe del incidente, constando ya el log con la URL utilizada en el ataque, el detalle de los datos personales extraídos y la estructura de tablas afectadas.
- Este mismo día ya se ha determinado la clasificación del incidente de seguridad, nivel de peligrosidad y declaración de la brecha de protección de datos, concluyéndose la conveniencia de notificar ante AEPD.

- La brecha se comunica a esta Agencia el día 7 de diciembre de 2021, martes. Justifican el retraso de la notificación tardía indicando que “el plazo de 72h expira fuera de la jornada laboral, durante el fin de semana o en vacaciones”.

CONCLUSIONES

1. Según el informe interno que el responsable realiza del incidente, se valora el nivel de riesgo para los derechos y libertades de las personas afectadas como ALTO, concluyendo que es necesario notificar a la AEPD, pero que NO existe necesidad de comunicar la brecha al ciudadano, indican que han utilizado la herramienta COMUNICA-BRECHA RGPG, pero no han obtenido un resultado concluyente al respecto. En el transcurso de esta investigación se ha utilizado esta herramienta con los datos aportados en la notificación de la brecha, obteniéndose como resultado la necesidad de comunicar la brecha a los afectados.

2. No disponen de análisis de riesgos para las actividades de tratamientos de datos personales afectados por la brecha. Justifican que, para todas las actividades de tratamientos con datos personales no sensibles, fundamentalmente datos identificativos, se cubren con la línea de controles generales aplicados a distintos niveles dentro de la organización, tanto en el marco organizativo como operacional y técnico.

3. Existen medidas de seguridad preventivas, pero no se corresponden con todas las medidas de seguridad previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero de 2010, por el que se regulaba el Esquema Nacional de Seguridad en el momento de producirse la brecha (derogado recientemente por el Real Decreto 311/2022, de 3 de mayo de 2022). Se reconoce el incumplimiento de algunas de estas medidas.

4. No disponen de auditoría de seguridad conforme a las previsiones del Esquema Nacional de Seguridad para el sistema de información indicado, esta auditoría es obligatoria según la normativa que regula este Esquema.

5. Se muestra diligencia y rapidez en el proceso interno de análisis y gestión del incidente, se documenta un informe muy completo y detallado del mismo, se acude al soporte del responsable de Seguridad de la Información (servicio de Protección de Datos y Seguridad de la Información) para evaluar el nivel de peligrosidad de la brecha. En este proceso de análisis interno se contacta con organismos de ciberseguridad en España, tales como INCIBE y CCN CERT, se interpone también denuncia ante el Cuerpo Nacional de Policía.

TERCERO: En fecha 27 de diciembre de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 del RGPD, y por las presuntas infracciones de los artículos 32 del RGPD y 34 del RGPD, tipificadas en el artículo 83.4 del RGPD.

El acuerdo de inicio fue enviado, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibido en fecha 28 de diciembre de 2022, como consta en el certificado que obra en el expediente.

CUARTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la entidad investigada presentó escrito de alegaciones en el que, en síntesis, manifestaba respecto de los datos afectados, que la afectación y naturaleza de los mismos no se corresponde en todos los casos con personas físicas y, en ningún caso, con información sensible, datos de menores, financieros, etc., o cualesquiera otros susceptibles de ser utilizados para operaciones fraudulentas.

Con relación al número de IPs desde las que se produjo el ataque, en la notificación de la brecha de datos personales realizada a la Agencia, se aportaba un informe técnico que precisaba decenas de direcciones IP desde las que se había efectuado ataque.

En relación con la cronología de los hechos recogidos, se indica que desde que se tiene conocimiento de la posible violación de datos, se establecieron contactos para la gestión del incidente con el Cuerpo Nacional de Policía, INCIBE y con el Centro Criptológico Nacional a través de la apertura del correspondiente incidente y se adoptaron medidas para eliminar el posible riesgo.

Asimismo, expone que no se tiene conocimiento de la utilización por terceros de los datos que, en su caso, pudieran haberse obtenido.

En relación con el análisis del riesgo de la brecha de datos, se indica que se va a desarrollar un nuevo procedimiento de comunicación de brechas de datos personales para que se ajuste -exactamente- a la terminología y escalas recogidas en RGPD y LOPDGDD, así como en la Guía para la notificación de Brechas de Datos Personales de esa Agencia y de la Guía WP250 (GT29) de Directrices sobre la notificación de las violaciones de la seguridad de los datos personales, de acuerdo con el Reglamento 2016/679.

Añade que está previsto el desarrollo de una nueva aplicación para la Gestión de la Privacidad y Seguridad de la Información en la Administración de la Comunidad Autónoma de Extremadura, que además ***(...)*** y que se sigue trabajando actualmente en el mantenimiento correctivo y adaptativo del desarrollo y revisión completa de las actividades de tratamiento de datos implicadas en el sistema de información, que ha propiciado la puesta en marcha de un nuevo desarrollo que corrige las vulnerabilidades que motivaron la brecha.

En relación con el uso de la herramienta COMUNICA-BRECHA RGPD y resultado comunicado en respuesta al requerimiento de 18 de mayo de 2022, y diferencias en el resultado con los aportados en la notificación de acuerdo de inicio de sancionador de 28 de diciembre de 2022, se reconoce que efectivamente existen diferencias que,

según se ha podido comprobar provienen de dos variaciones en los parámetros de utilización de dicha herramienta.

Por otro lado, manifiesta que, en el contrato licitado y adjudicado a nivel general para la gestión de la privacidad y seguridad de la información, han incorporado específicamente en las primeras etapas de ejecución del contrato y dentro del análisis de riesgos, tareas específicas de detección de vulnerabilidades técnicas, ataques externos / internos, pentesting, etc. como tareas que ayuden a identificar esta problemática.

Se insiste en que en la Administración de la Comunidad Autónoma gestiona la seguridad de la información y la protección de datos, si bien resulta posible que existan fallos en la implantación de controles y medidas de protección como ha sucedido en este caso. Estos incidentes se gestionan con diligencia para aplicar medidas correctivas de mitigación de impacto y aquellas preventivas que les ayuden a mejorar y con el compromiso de mejorar todos los procesos que puedan ayudar a prevenir incidentes como el que resulta objeto de análisis.

En relación con los Fundamentos de Derecho y tipificación recogidos en el Acuerdo de Inicio se indica que no debe iniciarse procedimiento sancionador a la Consejería de Educación y Empleo – Junta de Extremadura, al no corresponderse ninguna de las circunstancias acaecidas con los supuestos de infracciones regulados en los preceptos en que se motiva el acuerdo de inicio de procedimiento sancionador.

Considera que no existe una presunta infracción del artículo 5.1.f) RGPD, puesto que queda patente la gestión de la seguridad de la información y protección de datos realizada por esa Administración, a pesar de que puedan existir fallos que propicien la explotación de algunas vulnerabilidades que fueron detectadas y gestionadas.

En base a lo anterior, no considera que exista presunta infracción del artículo 32 RGPD, dado que se habían adoptado medidas, pero algunas fallaron.

Asimismo, no se considera la infracción del artículo 34 RGPD, al no darse ninguna de las circunstancias para la comunicación a los interesados. Expone que la tipificación recogida en el acuerdo respecto del presente supuesto no se compadece con la realidad de la tramitación realizada, puesto que no se tiene conocimiento de requerimiento formulado por esa Autoridad de Control para la comunicación a los interesados respecto del incidente notificado a esta Agencia el 7 de diciembre de 2021.

Al informe de alegaciones firmado por la Dirección General de Innovación e Inclusión Educativa, se acompaña el escrito de respuesta de fecha 1 de junio de 2022, el análisis del incidente de seguridad de 03 de diciembre de 2021 y la denuncia presentada ante la Comisaría de la Policía Nacional, de 07 de diciembre de 2021.

QUINTO: En fecha 3 de febrero de 2023, se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se imponga a CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S06110011,

-por una infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD, una sanción de apercibimiento.

- por una infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 73 f) de la LOPDGDD, una sanción de apercibimiento.

-por una infracción del artículo 34 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 74 ñ) de la LOPDGDD, una sanción de apercibimiento

-y ordene la comunicación de la brecha de seguridad a los afectados en las condiciones establecidas en el artículo 34 RGPD, así como la implantación de las medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares.>>

La citada propuesta de resolución fue enviada, conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, siendo recibida en fecha 6 de febrero de 2023, como consta en el certificado que obra en el expediente.

SEXTO: En fecha 20 de febrero de 2023, la entidad investigada presentó escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, reitera el contenido de las alegaciones expresadas en el escrito de contestación al acuerdo de inicio del expediente sancionador, entendiendo que los hechos sobre los que se formulan las infracciones resultan suficientemente explicados y razonados, demostrando una actuación diligente por parte de esa Consejería, ya que una vez que los mismos se producen, son denunciados ante la Policía Nacional y comunicados a esta Agencia de Protección de Datos, motivos suficientes para considerar que las infracciones no se han cometido, debiéndose exonerar, por tanto, de la responsabilidad imputada.

En lo que especta a la celeridad de las actuaciones y presunta caducidad del procedimiento, manifiesta que las actuaciones previas habrían de entenderse caducadas toda vez que entre la fecha de notificación y acuse de recibo del incidente (7 de diciembre y 13 de diciembre de 2021, respectivamente) y Acuerdo de inicio del Procedimiento Sancionador (28 de diciembre de 2022), el período en que se llevan a cabo la citadas actuaciones, superaría ampliamente los 12 meses de plazo que recoge la LOPDGDD, como duración máxima para las mismas.

Asimismo, no considera que exista una presunta infracción del artículo 5.1.f) RGPD, puesto que queda patente la gestión de la seguridad de la información y protección de datos realizada, a pesar de que puedan existir fallos que propicien la explotación de algunas vulnerabilidades que fueron detectadas y gestionadas.

En base a lo anterior, no se considera que exista presunta infracción del artículo 32 RGPD, remitiéndose a todo lo ya expuesto en las alegaciones.

No se considera la infracción del artículo 34 RGPD, al no concurrir las circunstancias para la comunicación a los interesados. No se tiene conocimiento de requerimiento

formulado por esa Autoridad de Control para la comunicación a los interesados respecto del incidente notificado a esa Agencia el 7 de diciembre de 2021, hasta la propuesta de Resolución de febrero de 2023. El hecho de ordenar la comunicación de la brecha a los afectados ahora y en el momento de emitir la Propuesta de Resolución, desvirtúa una posible infracción del artículo 34 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 74 ñ) de la LOPDGDD, y es que no existe requerimiento previo de esa parte hacia esta Administración para realizar la comunicación a los interesados.

Respecto a la propuesta de ordenar la comunicación de la brecha de seguridad a los afectados en las condiciones establecidas en el artículo 34 RGPD expone que:

-Que es ahora, en 2023, en la notificación de propuesta de resolución de procedimiento sancionador que hace esta Autoridad de Control a esa Administración Autonómica, cuando solicita -por primera vez- la comunicación a los interesados de una violación de datos producida en 2021, cuando ni siquiera consta materialización de riesgos para los interesados derivados de la misma y, en cualquier caso, no compartiendo esta Administración que dicho riesgo tenga la consideración de Alto conforme a la escala manejada en la normativa reguladora.

- Que debería ponderarse el hecho de que esta Administración detectó y controló el incidente en menos de una semana, incluyendo las necesarias comunicaciones a Fuerzas y Cuerpos de Seguridad del Estado, Entidades especializadas y a esa Autoridad de Control, habiendo sido siempre proactiva en las decisiones y acciones llevadas a cabo en relación con la adopción de medidas técnicas y organizativas apropiadas para mejorar la seguridad de la información y la protección de datos personales.

- Que esta Administración entiende, por tanto, que tal comunicación en este momento generaría una alarma social y falta de confianza en esta Administración, por parte de sus propios empleados y ciudadanía.

-Que el requerimiento a esta Administración de comunicar a los afectados, una vez superado ampliamente el plazo para llevar a cabo las Actuaciones previas, generaría indefensión en esta Administración Autonómica en su calidad de interesada en el Procedimiento Sancionador y, lo que es aún peor, una alarma social que no se compadece con la naturaleza y características de la violación, ni con la ausencia de constancia de materialización de riesgos derivados de la misma.

Por último, alega que ha llevado a cabo, y sigue, con la implantación de medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, como es el desarrollo de una versión de la aplicación concernida que elimina las vulnerabilidades explotadas en esta brecha. También se ha lanzado un ambicioso plan para la mejora de la protección de datos y seguridad de la información, a través de la adjudicación y formalización de un contrato para la “definición, desarrollo, implantación, operación y mejora continua del sistema de gestión de la privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura”, expte. ***XXXXXXXXXX***, resultando crucial dicho procedimiento para mejorar procesos como los que en este caso han podido fallar.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: En fecha 21 de febrero de 2022, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de datos personales remitido por la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S0611011, relativo a un ciber incidente que afectó a la confidencialidad de datos personales de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, en algunos casos con credenciales de acceso. Asimismo, se tiene conocimiento de la venta de datos que tiene que ver con aplicativos e información gestionada desde el Servicio de Tecnologías de la Educación.

SEGUNDO: De la información aportada se desprende ***(…).***

TERCERO: Se han visto comprometidos datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto. NIF, Apellidos, Nombre, Teléfono, Dirección Postal, Email, Sexo, Jubilado, Discapacidad (datos parciales). Contraseñas de 18 cuentas institucionales de Educarex (el portal educativo de la Junta de Extremadura) y contraseñas ***(XXXXXXXX)*** de usuarios de gestión de la aplicación (no se especifica el número).

Volumen: 60000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma.

CUARTO: La entidad investigada no ha comunicado la brecha de seguridad y sus posibles efectos adversos a los afectados.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Cuestiones previas

La Consejería de Educación y Empleo de la Junta de Extremadura, como cualquier otra entidad pública, está obligada al cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos -RGPD-, y de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales -LOPDGDD- con respecto a los tratamientos de datos de carácter personal que realicen, entendiendo por dato de carácter personal, *"toda información sobre una persona física identificada o identificable*".

Se considera persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Asimismo, debe entenderse por tratamiento "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

Teniendo en cuenta lo anterior, la Consejería de Educación y Empleo de la Junta de Extremadura presta una serie de servicios públicos, para los cuales trata datos de carácter personal de sus empleados y ciudadanos.

Realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD:

«responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.*

El artículo 4 apartado 12 del 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, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad que afectó a la confidencialidad de datos personales de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, y en algunos casos a credenciales de acceso almacenadas con un sistema de hash considerado débil, viéndose afectados datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto. NIF, Apellidos, Nombre, Teléfono, Dirección Postal, Email, Sexo, Jubilado, Discapacidad (datos parciales). Contraseña de 18

cuentas institucionales de Educarex y contraseñas ***(XXX)*** de usuarios de gestión de la aplicación (no especifica el número).

Según el GT29 se produce una "Violación de la confidencialidad" cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Alegaciones Aducidas al Acuerdo de Inicio

En respuesta a las alegaciones presentadas por la entidad investigada se debe señalar lo siguiente:

Alega la entidad investigada que no existe una presunta infracción del artículo 5.1.f) RGPD, puesto que queda patente la gestión de la seguridad de la información y protección de datos realizada por esa Administración, a pesar de que puedan existir fallos que propicien la explotación de algunas vulnerabilidades que fueron detectadas y gestionadas.

A este respecto, procede señalar que en el caso que nos ocupa, se produjo una brecha de seguridad provocada por un ciber incidente que afectó a la confidencialidad de datos personales de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, viéndose afectados datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto, NIF, apellidos, nombre, teléfono, dirección postal, Email, sexo, jubilado, discapacidad (datos parciales), contraseñas de 18 cuentas institucionales de Educarex (el portal educativo de la Junta de Extremadura) y contraseñas de usuarios de gestión de la aplicación. Ello unido a la publicación en Internet de un exiguo anuncio de venta de datos, supone sin duda alguna una vulneración de la confidencialidad de los datos personales. Lo relevante para entender vulnerada la confidencialidad es que la información se encontró totalmente a la libre disposición de terceros no autorizados. El hecho de que no conste una utilización posterior de los datos no desvirtúa el hecho de que se haya producido un acceso no autorizado.

En este sentido, es importante el hecho de que fueran objeto de pérdida de confidencialidad, la contraseña de 18 cuentas institucionales de Educarex y contraseñas de usuarios de gestión de la aplicación. A este respecto, debe señalarse que la pérdida de confidencialidad de credenciales de acceso implica, a su vez, la posibilidad que se acceda a otros múltiples datos personales tras el acceso a las aplicaciones.

Por tanto, no puede defenderse de ninguna manera que no exista una infracción del artículo 5.1.f) RGPD, puesto que, al no haberse adoptado medidas de seguridad adecuadas, los datos personales estuvieron accesibles.
El deber de confidencialidad resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española.

En efecto, este precepto contiene un "instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (Sentencia del Tribunal Constitucional 292/2000, de 30/11).

Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

En el caso que nos ocupa, ha quedado acreditado que la parte reclamada ha vulnerado este deber de confidencialidad en relación con los datos personales afectados.

Esta información no puede ser facilitada a terceros, salvo consentimiento de los usuarios o que exista una habilitación legal que permita su comunicación, circunstancias que no concurren en el presente caso. Todo ello supone una infracción del artículo 5.1. f) del RGPD al haber posibilitado, por la ausencia de medidas de protección, que terceras personas puedan tener acceso a datos personales contenidos en la base de datos.

En todo caso, en esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional en su Sentencia de 11/12/2008 (recurso 36/08), en la que indica lo siguiente:

"… la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor."

Alega también la entidad investigada que la Administración de la Comunidad Autónoma gestiona la seguridad de la información y la protección de datos, si bien resulta posible que existan fallos en la implantación de controles y medidas de protección como ha sucedido en este caso. Estos incidentes se gestionan con diligencia para aplicar medidas correctivas de mitigación de impacto y aquellas preventivas que ayuden a mejorar.

Frente a ello, procede señalar que, tal y como ya se indicó en el Acuerdo de Inicio del presente procedimiento sancionador, las medidas de seguridad no se estaban cumpliendo en el momento de los hechos.

En este sentido, no disponían de análisis de riesgos para las actividades de tratamientos de datos personales afectados por la brecha ni de auditoría de seguridad conforme a las previsiones del Esquema Nacional de Seguridad para el sistema de información indicado. Esta auditoría es obligatoria según la normativa que regula este Esquema.

Existían medidas de seguridad preventivas, pero no se correspondían con todas las medidas de seguridad previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero de 2010, por el que se regulaba el Esquema Nacional de Seguridad en el momento de producirse la brecha (derogado recientemente por el Real Decreto 311/2022, de 3 de mayo de 2022). Se reconoce el incumplimiento de algunas de estas medidas.

Por tanto, de todo ello se deduce una falta de la debida diligencia tanto en el cumplimiento de las medidas de seguridad establecidas, así como en la supervisión o comprobación de su observancia y/o de la idoneidad de estas.

A este respecto, se señala que el artículo 32 del RGPD se infringe tanto si no se adoptan por el responsable las medidas de índole técnica y organizativas apropiadas que garanticen la seguridad de los datos personales, como si, establecidas éstas, las mismas no se observan.

Se entiende que las medidas de seguridad implantadas eran insuficientes, susceptibles de ser mejoradas; lo que se pone de manifiesto con la afirmación de la parte reclamada de que los mecanismos son mejorables y, de hecho, ya se han relacionado algunas acciones llevadas a cabo para su mejora, como contratar soporte externo especializado, entre otras.

Por último, en cuanto a la infracción del artículo 34 del RGPD, tal y como se indicó en el Acuerdo de Inicio del presente procedimiento sancionador, en el transcurso de la investigación, el inspector utilizó la herramienta COMUNICA-BRECHA RGPG, con los datos aportados en la notificación de la brecha, obteniéndose como resultado la necesidad de comunicar la brecha a los afectados.

En concreto, la información utilizada como entrada en esta herramienta ha sido:

- Incidente intencionado, externo y consecuente de un ciberincidente.
- Personas u organizaciones no autorizadas han podido acceder y extraer datos.
- Los datos no estaban cifrados.
- Las personas afectadas pueden encontrar inconvenientes importantes, produciendo daño limitado, que podrán superar a pesar de algunas dificultades.
- No se tiene constancia de la materialización de alguno de los daños identificados.
- La probabilidad de materialización es baja.
- Los datos son (básicos, documento identificativo, de contacto, credenciales de acceso.
- No hay menores entre los afectados y se desconoce la existencia de colectivos vulnerables.
- La brecha afecta a unas 60000 personas, se detecta el 2 de diciembre de 2021, siendo la fecha de inicio aproximada el 29 de noviembre de 2021.”

Hay que tener en cuenta las graves consecuencias que puede tener en los derechos y libertades de los afectados, la filtración de datos de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, como son sus datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto, NIF, apellidos, nombre, teléfono, dirección postal, Email, sexo, jubilado, discapacidad (datos parciales), contraseñas de 18 cuentas institucionales de Educarex (el portal educativo de la Junta de Extremadura) y contraseñas de usuarios de gestión de la aplicación.

A este respecto el mencionado artículo 34 establece que cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

IV
Alegaciones Aducidas a la Propuesta de Resolución

En respuesta a las alegaciones presentadas por la entidad investigada a la Propuesta de Resolución, se debe señalar lo siguiente:

En lo que respecta a la celeridad de las actuaciones y presunta caducidad del procedimiento, manifiesta que las actuaciones previas habrían de entenderse caducadas toda vez que entre la fecha de notificación y acuse de recibo del incidente

(7 de diciembre y 13 de diciembre de 2021, respectivamente) y Acuerdo de inicio del Procedimiento Sancionador (28 de diciembre de 2022), el período en que se llevan a cabo la citadas actuaciones, superaría ampliamente los 12 meses de plazo que recoge la LOPDGDD, como duración máxima para las mismas.

El planteamiento que la entidad investigada realiza sobre esta cuestión en sus alegaciones no se ajusta a Derecho.

En el presente supuesto, el cómputo de los doce meses de duración máxima de las actuaciones previas AI/00120/2022, se inició el día 21 de febrero de 2022, fecha del acuerdo por el que se decide su iniciación, por lo que no se observa que, desde dicha fecha hasta la fecha del acuerdo de inicio del presente procedimiento sancionador, esto es, el 27 de diciembre de 2022, haya transcurrido el plazo de doce meses indicado en el artículo 67 de la LOPDGDD.

Por otra parte, debe señalarse que el plazo de caducidad del presente procedimiento, establecido en nueve meses, se computa desde la fecha en que se acuerda su inicio, resultando improcedente añadir a ese cómputo, a efectos de medir la duración del expediente administrativo, ningún otro período, tal como el tiempo de las actuaciones previas de investigación, o el tiempo que transcurra entre la finalización de esas actuaciones y la apertura del procedimiento, ni el tiempo correspondiente a la fase de admisión a trámite de las reclamaciones presentadas.

Así lo ha declarado repetidamente nuestro Tribunal Supremo. En Sentencia de 21/10/2015 se cita la Sentencia de 26/12/2007 (recurso 1907/2005), que declara lo siguiente:

“[…] el plazo del procedimiento […] se cuenta desde la incoación del expediente sancionador, lo que obviamente excluye del cómputo el tiempo de la información reservada";" […] la mayor o menor duración de la fase preliminar no lleva aparejada la caducidad del procedimiento ulterior".

También en Sentencia del Tribunal Supremo de 13/10/2011 (recurso 3987/2008) que examina un motivo de casación relativo al cómputo del plazo de caducidad del procedimiento, se declara lo siguiente:

“No podemos compartir el razonamiento que expone la Sala de instancia para fijar un dies a quo diferente al establecido por la Ley, señalando como fecha inicial del cómputo el día siguiente a la finalización de las diligencias previas informativas.
[…]
Pues bien, una vez realizadas esas actuaciones previas, el tiempo que tarde la Administración en acordar la incoación del procedimiento […] podrá tener las consecuencias que procedan en cuanto al cómputo de la prescripción (extinción del derecho); pero no puede ser tomado en consideración a efectos de la caducidad, pues esta figura lo que pretende es asegurar que una vez iniciado el procedimiento la Administración no sobrepase el plazo de que dispone para resolver. En el fundamento tercero de la sentencia recurrida la Sala de instancia realiza una interpretación de la norma que no es acorde con la naturaleza de la institución de la caducidad, pues a diferencia de la prescripción, que es causa de extinción del derecho o de la responsabilidad de que se trate, la caducidad es un modo de terminación del procedimiento por el transcurso del plazo fijado en la norma, por lo que su apreciación

no impide, si no ha transcurrido el plazo establecido para la prescripción de la acción de restablecimiento de legalidad urbanística por parte de la Administración, la iniciación de un nuevo procedimiento".

En cuanto a las manifestaciones efectuadas en relación con las infracciones imputables a la entidad investigada por la vulneración de los artículos 5.1.f), 32 y 34 de RGPD, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en el Fundamento de Derecho III de la Propuesta de Resolución y que reproducen en el Fundamento de Derecho III de esta Resolución.

Respecto a la propuesta de ordenar la comunicación de la brecha de seguridad a los afectados en las condiciones establecidas en el artículo 34 RGPD, se ofrece adecuado estimar la alegación en atención a las circunstancias del caso concreto y habida cuenta del tiempo transcurrido desde que tuvo lugar el incidente, dada la escasa utilidad práctica que tendría requerir ahora que se realizara la comunicación a los afectados.

En cuanto a las medidas correctoras que la entidad investigada manifiesta estar implantando para adecuar su actuación a la normativa de protección de datos personales, como es el desarrollo de una versión de la aplicación concernida que elimina las vulnerabilidades explotadas en esta brecha y el lanzamiento de un ambicioso plan para la mejora de la protección de datos y seguridad de la información, a través de la adjudicación y formalización de un contrato para la "definición, desarrollo, implantación, operación y mejora continua del sistema de gestión de la privacidad y seguridad de la información de la Administración de la Comunidad Autónoma de Extremadura", aunque refleja una conducta positiva, no desvirtúa los hechos constatados.

No obstante, esta Agencia valora positivamente la adopción de nuevas medidas que redunden en una mayor seguridad en lo que al tratamiento de datos personales se refiere y que puedan prevenir, en un futuro, incidentes como el que se sustancia en el presente procedimiento.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de las infracciones que se declaran cometidas ni suponen causa de justificación o exculpación suficiente.

V

Artículo 5.1.f) del RGPD

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

1. Los datos personales serán:

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra

su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).”

En relación con este principio, el Considerando 39 del referido RGPD señala que:

“[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento”.

La documentación obrante en el expediente ofrece indicios evidentes de que la entidad investigada vulneró el artículo 5.1 f) del RGPD, *principios relativos al tratamiento* toda vez que a raíz de la brecha de confidencialidad, los datos personales de 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, obrantes en el sistema fueron indebidamente expuestos a terceros, y en algunos casos afectando a credenciales de acceso ***(…),*** vulnerando los principios de integridad y confidencialidad, ambos establecidos en el citado artículo 5.1.f) del RGPD.

En consecuencia, se considera que los hechos acreditados son constitutivos de infracción, imputable a la entidad investigada, por vulneración del artículo 5.1.f) del RGPD.

VI
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD, supone la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *“Condiciones generales para la imposición de multas administrativas”* dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)”*

A este respecto, la LOPDGDD, en su artículo 71 “*Infracciones*” establece que *“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”*.

A efectos del plazo de prescripción, el artículo 72 “*Infracciones consideradas muy graves*” de la LOPDGDD indica:

“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) *El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

VII
Artículo 32 del RGPD

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

Los hechos puestos de manifiesto suponen la falta de medidas técnicas y organizativas al posibilitar la exhibición de datos de carácter personal de los usuarios con la consiguiente falta de diligencia por el responsable, permitiendo el acceso no autorizado por terceros ajenos.

En el caso concreto que se examina, ***(…).***
Por tanto, se considera que existen evidencias suficientes respecto de la ausencia de medidas de seguridad adecuadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento.

Por otra parte, no disponen de análisis de riesgos para las actividades de tratamientos de datos personales afectados por la brecha. Tampoco disponen de auditoría de seguridad conforme a las previsiones del Esquema Nacional de Seguridad para el sistema de información indicado. Esta auditoría es obligatoria según la normativa que regula este Esquema.

Existen medidas de seguridad preventivas, pero no se corresponden con todas las medidas de seguridad previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero de 2010, por el que se regulaba el Esquema Nacional de Seguridad en el momento de producirse la brecha (derogado recientemente por el Real Decreto 311/2022, de 3 de mayo de 2022). Se reconoce el incumplimiento de algunas de estas medidas.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados:

"Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

En este sentido, la búsqueda en internet, por ejemplo, del nombre, apellidos, DNI o correo electrónico de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

En consecuencia, se considera que los hechos acreditados son constitutivos de infracción, imputable a la entidad reclamada, por vulneración del artículo 32 RGPD.

VIII

Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD, supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica"*.

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."

IX
Artículo 34 del RGPD

El artículo 34 "Comunicación de una violación de la seguridad de los datos personales al interesado" del RGPD establece:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

1. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3".

En el presente caso, según el informe interno que el responsable realiza del incidente, se valora el nivel de riesgo para los derechos y libertades de las personas afectadas como ALTO, concluyendo que es necesario notificar a la AEPD, pero que NO existe necesidad de comunicar la brecha al ciudadano. Indican que han utilizado la herramienta COMUNICA-BRECHA RGPG, pero no han obtenido un resultado concluyente al respecto.

Pues bien, en el transcurso de la investigación el inspector ha utilizado esta herramienta con los datos aportados en la notificación de la brecha, obteniéndose como resultado la necesidad de comunicar la brecha a los afectados.

En concreto, la información utilizada como entrada en esta herramienta ha sido:

- Incidente intencionado, externo y consecuente de un ciberincidente.
- Personas u organizaciones no autorizadas han podido acceder y extraer datos.
- Los datos no estaban cifrados.
- Las personas afectadas pueden encontrar inconvenientes importantes, produciendo daño limitado, que podrán superar a pesar de algunas dificultades.
- No se tiene constancia de la materialización de alguno de los daños identificados.
- La probabilidad de materialización es baja.
- Los datos son (básicos, documento identificativo, de contacto, credenciales de acceso.
- No hay menores entre los afectados y se desconoce la existencia de colectivos vulnerables.
- La brecha afecta a unas 60000 personas, se detecta el 2 de diciembre de 2021, siendo la fecha de inicio aproximada el 29 de noviembre de 2021.

Hay que tener en cuenta las graves consecuencias que puede tener en los derechos y libertades de los afectados, la filtración de datos de aproximadamente 60.000 usuarios con la categoría de personal docente preuniversitario de la Comunidad Autónoma, como son sus datos básicos, identificativos (NIF, NIE o Pasaporte), localización y contacto, NIF, apellidos, nombre, teléfono, dirección postal, Email, sexo, jubilado, discapacidad (datos parciales), contraseñas de 18 cuentas institucionales de Educarex (el portal educativo de la Junta de Extremadura) y contraseñas de usuarios de gestión de la aplicación.

A este respecto el mencionado artículo 34 establece que cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

En consecuencia, se considera que los hechos acreditados son constitutivos de infracción, imputable a la entidad investigada, por vulneración del artículo 34 RGPD.

X
Tipificación de la infracción del artículo 34 del RGPD

La citada infracción del artículo 34 del RGPD, supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "Condiciones generales para la imposición de multas administrativas" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 74 "Infracciones consideradas leves" de la LOPDGDD indica:

"*Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*

"(…)

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica. (…)"

XI
Sanción

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.*"

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

(…)

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a

las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica."

En el presente caso, de las sólidas evidencias de las que se dispone conforme a los hechos probados en el presente procedimiento sancionador, se estima adecuado sancionar con apercibimiento a la entidad investigada, por infracción del artículo 5.1.f) del RGPD, por la infracción del artículo 32 del RGPD, y por infracción del artículo 34 del RGPD, por la falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad, así como por el incumplimiento del deber de comunicación a los afectados de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los mismos.

XI
Adopción de Medidas

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: SANCIONAR con APERCIBIMIENTO a la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S06110011, por una infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD.

SEGUNDO: SANCIONAR con APERCIBIMIENTO a la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S06110011, por una infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 73 f) de la LOPDGDD.

TERCERO: SANCIONAR con APERCIBIMIENTO a la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S06110011, por una infracción del artículo 34 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 74 ñ) de la LOPDGDD.

CUARTO: REQUERIR a la CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA, con NIF S06110011, que implante, en el plazo de tres meses, las

medidas correctoras necesarias para adecuar su actuación a la normativa de protección de datos personales, que impidan que en el futuro se repitan hechos similares, así como que informe a esta Agencia en el mismo plazo sobre las medidas adoptadas.

QUINTO: NOTIFICAR la presente resolución a CONSEJERÍA DE EDUCACIÓN Y EMPLEO - JUNTA DE EXTREMADURA.

SEXTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

Mar España Martí
Directora de la Agencia Española de Protección de Datos