- **Expediente N.º: EXP202200993**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante), en fecha 15 de diciembre de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la CONSEJERIA DE EDUCACION Y FORMACION PROFESIONAL DEL GOBIERNO DE ILLES BALEARS, con NIF S0711001H (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

El reclamante manifiesta que durante el curso académico 2020/2021, estuvo ejerciendo de profesor en el IES ***IES.1***, de ******LOCALIDAD.1*** (Illes Balears), siéndole asignada una dirección de correo electrónico corporativo a la que dejó de tener acceso al finalizar el curso académico. No obstante, en fecha 15 de diciembre de 2021, recibió comunicación de GOOGLE informándole de un nuevo inicio de sesión en la referida cuenta corporativa por lo que considera que podría haberse suplantado su identidad y vulnerado sus derechos en torno a la protección de datos.

Junto a la notificación aporta captura de pantalla del mensaje recibido de GOOGLE alertando del inicio de sesión en la cuenta.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó mediante notificación electrónica, 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), fue recibido en fecha 4 de febrero de 2022, como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: En fecha 15 de marzo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se comunica la admisión a trámite de la reclamación presentada por la parte reclamante.

CUARTO: 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:

Durante las presentes actuaciones se han investigado las siguientes entidades:

CONSEJERÍA DE EDUCACIÓN Y FORMACIÓN PROFESIONAL DEL GOBIERNO DE ILLES BALEARS, con NIF S0711001H, y domicilio en CARRER DEL TER 16- 07009 PALMA (ILLES BALEARS).

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

El reclamante aporta una captura de pantalla con contenido en lengua catalana en la que GOOGLE informa que se ha producido un nuevo inicio de sesión en la cuenta ******EMAIL.1.***

En fecha 3 de mayo de 2022, se solicitó información en relación con los hechos denunciados a la CONSEJERÍA DE EDUCACIÓN Y FORMACIÓN PROFESIONAL DEL GOBIERNO DE ILLES BALEARS, sin obtener respuesta.

En fecha 14 de julio de 2022, se recibe respuesta al requerimiento de información de la Inspección de Datos, en el que se pone de manifiesto lo siguiente:

El reclamante ha sido docente del centro desde el día 1 de septiembre de 2020 hasta el 31 de agosto de 2021.

Durante los primeros días de septiembre, se le facilitó una dirección de correo electrónico corporativo, con finalidades exclusivamente académicas y profesionales relacionadas con el mencionado centro docente.

Se ha detectado que accidentalmente no se le retiró el acceso a su cuenta de correo electrónico en el mes de septiembre de 2021, como debería haberse hecho, que el centro no ha cambiado la contraseña de la dirección de correo electrónico del reclamante, en consecuencia, éste seguía teniendo acceso a ésta.

Se desconocen los motivos y personas que puedan haber tenido acceso a esta cuenta, y que en ningún caso ha sido con conocimiento y consentimiento del equipo directivo, que en todo momento se comunica al equipo docente que el uso de esta cuenta es exclusivo para tareas académicas, jamás de uso personal, ya que es propiedad de la administración educativa, y que como consecuencia de la detección de la no retirada de acceso a la cuenta de correo electrónico corporativo, se le retira el acceso.

Respecto a la documentación requerida sobre las políticas de seguridad del correo electrónico corporativo, normas de uso e información que se facilita a los empleados y usuarios y normas de cancelación de las cuentas de correo electrónico del personal cesante, manifiestan que se dispone de un sistema de seguridad denominado de doble verificación. Este sistema añade una capa de seguridad adicional en el caso de robo de contraseña y por seguridad envía un correo electrónico a la misma cuenta de

***URL.1** en el momento que detecta una entrada desde un dispositivo diferente del habitual. El sistema informa con un mensaje al titular de la cuenta para comprobar que no se trata de un intruso que pretende un acceso indebido.

CONCLUSIONES:

-El reclamante ha sido docente del centro desde el día 1 de septiembre de 2020 hasta el 31 de agosto de 2021, y como consecuencia se le facilitó una dirección de correo electrónico corporativo, con finalidades exclusivamente académicas y profesionales relacionadas con el mencionado centro docente.

-El día 15 de diciembre de 2021, hubo un acceso a la cuenta de correo corporativa del reclamante, desconociéndose los motivos y personas que puedan haber tenido acceso a esta cuenta.

-Como consecuencia de la detección de la no retirada de acceso a la cuenta de correo electrónico corporativo, a partir de esta reclamación, se le retira el acceso.

-No aportan documentación acreditativa de las políticas de seguridad del correo electrónico corporativo, normas de uso e información que se facilita a los empleados y usuarios y normas de cancelación de las cuentas de correo electrónico del personal cesante.

QUINTO: En fecha 23 de noviembre 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 32 del RGPD, tipificada 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 25 de noviembre de 2022, como consta en el certificado que obra en el expediente.

SEXTO: 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 parte reclamada presentó escrito de alegaciones en el que, en síntesis, aporta un informe técnico elaborado por el Servicio de Tecnologías de la Información en la Educación de la Dirección General de primera Infancia y Comunidad Educativa.

En dicho informe se pone de manifiesto que, en las Islas Baleares, los centros educativos tienen consolas propias ya sea de Google Workspace o de Microsoft (en el caso de un centro), debido a la necesidad que surgió durante la pandemia de poseer entornos digitales en los que poder continuar con la educación del alumnado ante los escenarios de confinamiento y semipresencialidad.

Desde la Consejería de Educación y Formación Profesional, a través del CEP IBSTEAM, se realizaron formaciones específicas para la gestión de estas consolas

educativas en las cuáles se plantearon las políticas de seguridad y protección de datos.

Asimismo, se indica que, ante la baja por cualquier motivo de un trabajador, las cuentas se suspenden, no se eliminan, a fin de que si el trabajador vuelve a estar en activo (situación frecuente en personal docente) pueda acceder a los correos electrónicos (con documentación de trabajo) de cursos anteriores.

No obstante, se recomienda que el tiempo entre el cese y la suspensión de la cuenta sea de un mes, si bien los centros educativos aplicaron una política más laxa en cuanto a fechas de suspensión de usuarios por las implicaciones de la pandemia de COVID-19 permitiendo un mayor tiempo a los docentes para transferir material a nuevas cuentas.

En relación con el caso concreto que ha generado la reclamación, manifiesta su sorpresa por la aceptación como prueba para tramitar la denuncia, de la captura de pantalla del correo electrónico en la que no consta la fecha.

El Servicio de Tecnologías de la Información en la Educación, con la colaboración del centro IES ***IES.1***, han comprobado la actividad de la cuenta mediante las herramientas de auditoría e investigación de la consola Workspace del IES ***IES.1***.

Resultado de dichas comprobaciones, considera necesario que se tenga en cuenta lo siguiente:

-A pesar de lo que manifiesta el reclamante, se observa que no ha habido ningún cambio de contraseña. Ni el propietario de la cuenta realizó nunca un cambio de esta desde el momento de la creación. Además, la única actividad posterior a la creación de la cuenta fue su suspensión con fecha 15 de junio de 2022.

-El reclamante, en contra de lo que manifiesta, mantuvo el acceso a la cuenta hasta junio de 2022. Los centros educativos aplicaron una política más laxa en cuanto a fechas de suspensión de usuarios por las implicaciones de la pandemia de COVID-19 permitiendo un mayor tiempo a los docentes para transferir material a nuevas cuentas.

-En lo que respeta a los accesos, existe un acceso de fecha 15 de diciembre de 2021, para realizar el cambio de propiedad de una clase de Classroom. Este acceso se realizó a petición por el propio reclamante. Al acceder a la aplicación Classroom, el aviso se produce de la misma forma que si fuera directamente a la aplicación de correo.

-El centro dispone de un protocolo de uso de las cuentas corporativas para las cuentas nuevas, aprobado en septiembre de 2022. Se aporta el protocolo original y su traducción. Con anterioridad a esta fecha la información se daba de forma oral.

Se aporta con este informe documentación acreditativa de las políticas de seguridad del correo corporativo, en las que se está trabajando a nivel de Consejería además de las propias del centro.

SÉPTIMO: En fecha 6 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 CONSEJERIA DE EDUCACION Y FORMACION PROFESIONAL DEL GOBIERNO DE LAS ISLAS BALEARES, con NIF S0711001H, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, una sanción de apercibimiento.>>

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.

OCTAVO: En fecha 14 de febrero de 2023, la parte reclamada presentó escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, manifiesta que:

Respecto del primer hecho declarado probado, en el que el reclamante considera que podría haberse suplantado su identidad y vulnerado sus derechos en torno a la protección de datos, alega que es una manifestación totalmente hipotética, puesto que tal y como consta en el Informe técnico de 13 de febrero de 2023, la comunicación que recibió el reclamante de Google en fecha 15 de diciembre de 2021, informándole de un nuevo inicio de sesión en su cuenta corporativa, solo prueba que recibió un aviso de alerta de seguridad de que se había detectado un intento de acceso a la cuenta que se realiza de forma automática por Google y que del análisis realizado a la consola del IES ***IES.1***, se observó que este intento de acceso se produjo por la acción realizada por el propio reclamante al hacer el cambio de propiedad en el Classroom.

Por tanto, solo hubo un acceso a su cuenta corporativa que fue el día 15 de diciembre de 2021, para realizar el cambio de propiedad de una clase de Classroom, y este acceso se realizó por el propio reclamante. En ningún momento se ha probado en el expediente sancionador que hubo un acceso real de otra persona a la cuenta del reclamante, ni que se haya suplantado su identidad.

Respecto del segundo hecho declarado probado, manifiesta que el Servicio de Tecnologías de la Información en la Educación con la colaboración del centro IES ***IES.1***, comprobaron la actividad de la cuenta mediante las herramientas de auditoría e investigación de la consola Workspace del IES ***IES.1***, resultando que no hubo ningún cambio de contraseña en la cuenta desde el momento de la creación, por parte del usuario ni del administrador, y así ha quedado registrado en la herramienta de auditoría de la consola de Google Workspace.

Respecto del tercer hecho declarado probado, indica que la no suspensión de la cuenta del reclamante, que mantuvo el acceso hasta junio de2022, en ningún caso implica un problema de seguridad, dado que se mantienen las medidas técnicas de la cuenta.

Expone que debe tomarse en consideración que la Consejería de Educación y Formación Profesional está aplicando medidas de mejora continua en cuanto a las políticas de seguridad y protección de datos. Así a través del CEP IBSTEAM, se han realizado formaciones específicas para la gestión de las consolas educativas Workspace desde el 2020. En este caso en concreto, el IES ***IES.1*** aprobó un Protocolo

de uso de la cuenta corporativa para el profesorado en septiembre de 2022, y actualmente se está trabajando en la unificación de todas las consolas en una sola, gestionada directamente por el Servicio de Tecnologías de la Información en Educación.

Alega que el hecho de que la Consejería se encuentre en un proceso de mejora para unificar la aplicación de medidas de seguridad no equivale a que la situación anterior supusiera un nivel de seguridad bajo. Por tanto, se puede afirmar que dichas cuentas de correo electrónico corporativo, cuyo uso es exclusivo para tareas académica por ser propiedad de la administración educativa, están dotadas de sistemas de seguridad suficientes y eficientes para evitar el acceso indebido de personas ajenas a las autorizadas en las cuentas de correo electrónico, al disponer de doble verificación para el acceso desde dispositivos diferentes del habitual.

Por todo lo expuesto anteriormente, considera que no se ha vulnerado lo dispuesto en el artículo 32 del RGPD, que a pesar de haberse producido un incidente de seguridad en sus sistemas, debido al hecho de que no se retiró al reclamante el acceso a su cuenta de correo electrónico como debería haberse hecho, al igual que pasó con otros usuarios ante las dificultades de la situación derivada de la pandemia de COVID 19, en ningún momento durante la tramitación del expediente sancionador se han probado los hechos imputados que integran la infracción por parte de la AEPD, y no aprecia que haya pruebas que sostengan el acceso a esta cuenta corporativa por parte de una tercera persona, ni que se haya suplantado su identidad, y por consiguiente, que realmente se haya producido un riesgo efectivo para las garantías de los derechos y libertades de los interesados en relación con el tratamiento de datos personales, por lo que solicita se proceda al archivo del expediente sancionador, con la consiguiente declaración de ausencia de responsabilidad.

Se aporta Informe Técnico del Servicio de Tecnologías de la Información en la Educación, de 13 de febrero de 2023.

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: Consta que en fecha 15 de diciembre de 2021, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, en la que ponía de manifiesto que durante el curso académico 2020/2021, estuvo ejerciendo de profesor en el IES ***IES.1***, de ******LOCALIDAD.1*** (Illes Balears), siéndole asignada una dirección de correo electrónico corporativo a la que dejó de tener acceso al finalizar el curso académico.

No obstante, en fecha 15 de diciembre de 2021, recibió comunicación de GOOGLE, informándole de un nuevo inicio de sesión en la referida cuenta corporativa por lo que considera que podría haberse suplantado su identidad y vulnerado sus derechos en torno a la protección de datos.

SEGUNDO: Consta en las actuaciones previas, que la AEPD requirió a la parte reclamada información relacionada con la incidencia, confirmándose lo señalado en el escrito de reclamación, al manifestar la parte reclamada que accidentalmente no se le retiró el acceso a su cuenta de correo electrónico como debería haberse hecho, y que el centro no cambió la contraseña de la dirección de correo electrónico del reclamante por lo que éste seguía teniendo acceso a ésta, desconociendo los motivos y personas que han podido tener acceso a la cuenta.

TERCERO: Del resultado de la comprobación de la actividad de la cuenta mediante herramientas de auditoría e investigación de la consola Workspace del IES ***IES.1***, efectuada por el Servicio de Tecnologías de la Información en la Educación, con la colaboración del centro IES ***IES.1*** consta que, el reclamante que fue docente del centro desde el día 1 de septiembre de 2020 hasta el 31 de agosto de 2021, mantuvo el acceso a la cuenta hasta junio de 2022, es decir, más de un mes después del cese del reclamante como docente del centro.

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 Formación Profesional del Gobierno de Illes Balears, 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.

En el caso concreto que se examina, la dirección de correo electrónico corporativa creada en el contexto de la actividad laboral, compuesta por el nombre y apellido de la persona a la que se le ha atribuido, constituye un dato de carácter personal en el sentido del artículo 4.1 del RGPD, y, por tanto, datos relacionados con una persona física identificada o identificable.

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 Formación Profesional del Gobierno de las Islas Baleares 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 lo que respecta a la aplicación de la normativa de protección de datos al supuesto planteado, debe tenerse en cuenta que el RGPD, en su artículo 32, exige a los responsables del tratamiento, la adopción de las correspondientes medidas de seguridad necesarias que garanticen que el tratamiento es conforme a la normativa vigente, así como garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, solo los pueda tratar siguiendo instrucciones del responsable.

III

Alegaciones Aducidas al Acuerdo de Inicio

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

Alega la parte reclamada que, ante la baja por cualquier motivo de un trabajador, las cuentas se suspenden, no se eliminan, a fin de que si el trabajador vuelve a estar en

activo (situación frecuente en personal docente) pueda acceder a los correos electrónicos (con documentación de trabajo) de cursos anteriores.

Asimismo, se indica la recomendación de que el tiempo entre el cese y la suspensión de la cuenta sea de un mes por lo que, en este sentido, procede señalar entonces que las medidas de seguridad no se estaban cumpliendo en el momento de los hechos.

Del resultado de la comprobación de la actividad de la cuenta mediante herramientas de auditoría e investigación de la consola Workspace del IES ***IES.1***, efectuada por el Servicio de Tecnologías de la Información en la Educación, con la colaboración del centro IES ***IES.1*** consta que, el reclamante, que fue docente del centro desde el día 1 de septiembre de 2020 hasta el 31 de agosto de 2021, mantuvo el acceso a la cuenta hasta junio de 2022, es decir, mucho más de un mes después del cese del reclamante como docente de dicho centro.

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.

De hecho, tal y como consta en las actuaciones previas, la AEPD requirió a la parte reclamada información relacionada con la incidencia, confirmándose lo señalado en el escrito de reclamación, al manifestar la parte reclamada que accidentalmente no se le retiró el acceso a su cuenta de correo electrónico como debería haberse hecho, y que el centro no cambió la contraseña de la dirección de correo electrónico del reclamante por lo que éste seguía teniendo acceso a ésta, desconociendo los motivos y personas que han podido tener acceso a la cuenta.

A este respecto, debe señalarse 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 que, hasta septiembre de 2022, el centro no dispuso de un protocolo de uso de las cuentas corporativas para las cuentas nuevas.

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 reclamada a la Propuesta de Resolución, se debe señalar lo siguiente:

Alega la parte reclamada que solo hubo un acceso a la cuenta corporativa que fue el día 15 de diciembre de 2021, para realizar el cambio de propiedad de una clase de Classroom, y este acceso se realizó por el propio reclamante y que en ningún momento se ha probado en el expediente sancionador que hubo un acceso real de

otra persona a la cuenta del reclamante, ni que se haya suplantado su identidad. Asimismo, manifiesta que no hubo ningún cambio de contraseña en la cuenta desde el momento de la creación, por parte del usuario ni del administrador, y así ha quedado registrado en la herramienta de auditoría de la consola de Google Workspace.

A este respecto, procede señalar que la apertura del presente Procedimiento Sancionador no se debió al acceso a la cuenta corporativa por parte de una tercera persona, o que se hubiere suplantado la identidad del reclamante, sino al hecho de haber tenido conocimiento de que se mantuvo el acceso a la cuenta hasta junio de 2022, es decir, mucho más de un mes después del cese del reclamante como docente del centro, a pesar de que la recomendación era que el tiempo entre el cese y la suspensión de la cuenta fuera de un mes.

Así, del análisis de la documentación aportada, la propia reclamada reconoce haberse producido un incidente de seguridad en sus sistemas, debido a que no se retiró al reclamante el acceso a su cuenta de correo electrónico como debería haberse hecho, al igual que pasó con otros usuarios ante las dificultades de la situación derivada de la pandemia de COVID 19. Es más, fue a partir de la reclamación, cuando se le retiró el acceso a la cuenta de correo electrónico corporativo.

En este sentido, debe recordarse que el 32 del RGPD, incide en la necesidad de que el responsable del tratamiento adopte medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos y garantizar un nivel de seguridad adecuado al riesgo, sin que pueda aceptarse como justificación la circunstancia de la emergencia sanitaria.

Aduce la parte reclamada que no se han probado los hechos imputados que integran la infracción. En este sentido, se significa que la responsabilidad proactiva conlleva que responsables y encargados tienen la obligación de cumplir con el RGPD y demostrar (acreditar) el cumplimiento del RGPD en el tratamiento de los datos personales, incluida la eficacia de las medidas, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

En este sentido el Considerando 74 establece que:

“Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.”

En el caso concreto que se examina, se constata que no se habían adoptado las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, toda vez que, hasta septiembre de 2022, el centro no dispuso de un protocolo de uso de las cuentas corporativas para las cuentas nuevas. De hecho, con anterioridad a esta fecha, la información se daba de forma oral.

Al continuar accediendo a la cuenta de correo electrónico, a su vez continúa pudiendo acceder a datos personales e información a la que ya no debería tener acceso por no

trabajar en ese centro. Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de estos datos.

En cuanto a las medidas de mejora continua que la Consejería manifiesta haber adoptado en cuanto a las políticas de seguridad y protección de datos, aunque refleja una conducta positiva, no desvirtúa los hechos constatados y que son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

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.

V
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;

a) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

a) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

b) 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 ten-

ga 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".

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."

De la documentación obrante en el expediente se ofrecen indicios evidentes de que la parte reclamada ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad en sus sistemas, al no retirar al reclamante acceso a su cuenta de correo electrónico como debería haberse hecho.

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 transmi-

tidos, 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".

En el presente caso, tal y como consta en las actuaciones previas, la AEPD requirió a la parte reclamada información relacionada con la incidencia, confirmándose lo señalado en el escrito de reclamación, al manifestar la parte reclamada que accidentalmente no se le retiró el acceso a su cuenta de correo electrónico como debería haberse hecho, y que el centro no cambió la contraseña de la dirección de correo electrónico del reclamante por lo que éste seguía teniendo acceso a ésta, desconociendo los motivos y personas que han podido tener acceso a la cuenta.

La responsabilidad de la parte reclamada viene determinada por la quiebra de seguridad puesta de manifiesto en la reclamación y documentación aportada, ya que es responsable de tomar las 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 parte reclamada, por vulneración del artículo 32 RGPD.

VI

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."

VII
Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de adopción de medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento constituye el elemento de la culpabilidad.

VIII
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 se estima adecuado sancionar con apercibimiento a la parte

reclamada, por la infracción del artículo 32 del RGPD, por la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.

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 CONSEJERIA DE EDUCACION Y FORMACION PROFESIONAL DEL GOBIERNO DE LAS ISLAS BALEARES, con NIF S0711001H, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a CONSEJERIA DE EDUCACION Y FORMACION PROFESIONAL DEL GOBIERNO DE LAS ISLAS BALEARES.

TERCERO: 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