

- **Expediente N.º: EXP202102527**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: A.A.A. (en adelante, la parte reclamante) con fecha 14/09/2021 interpuso una primera reclamación ante la Agencia Española de Protección de Datos, que amplía los días 14/12/2021 y 2/01/2022. Las reclamaciones se dirigen contra la **CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS-CEUCD**, con NIF S3511001D (en adelante, la parte reclamada).

Considera que la implantación de la plataforma GOOGLE SUITE PARA LA EDUCACIÓN (GS en lo sucesivo) no satisfacen ni se ajusta a los requisitos legales sobre protección de datos.

Refiere aspectos sucedidos desde el curso 2019-20 en el IES *****IES.1**(en lo sucesivo IES), donde se matriculó su hijo **B.B.B.**.

Enmarca la cronología de lo sucedido con la suscripción del Convenio de la CEUCD con GOOGLE IRELAND LIMITED BOC (19/10/2020) dentro del Plan para la educación digital, *“para el uso de GOOGLE SUITE PARA LA EDUCACIÓN en los centros docentes públicos dependientes de la CCAA de Canarias. “Para el curso 2021/2022, (9/09/2021), se facilitó a los padres de alumnos un modelo de consentimiento” informado “para el uso y tratamiento de “solución de servicios digitales y telemáticos para la comunicación y la colaboración GSUITE” en el link:*

*****URL.1”**

Según el reclamante: *“llevamos dos años donde se le ha dado de alta en una plataforma que ni siquiera nos ha solicitado autorización”, por decisión del IES y que con la suscripción del Convenio “Este año se han acogido al acuerdo de la Consejería de Educación donde en esta ocasión sí han solicitado autorización para el uso siguiendo las instrucciones de la Consejería. En los años anteriores a la suscripción del convenio por la Consejería no han solicitado ningún consentimiento informado, ni se han generado las actividades de tratamiento para su uso, sin realizar ninguna evaluación de las mismas en materia de seguridad de la información.”*

Aporta link de *“manual acogida 21/22” del IES, con “Índice”, dando clic en “GSUITE”, se accede al manual de acogida al curso 21-22 que contiene información sobre la plataforma GS para la Educación.*

Entre otros extremos, se indica que: *“G Suite Educativo es un paquete de herramientas y servicios de Google para centros educativos. Proporciona cuentas con un nombre de dominio personalizado por el cliente y ofrece servicios asociados,*

herramientas y aplicaciones web con funciones similares a las suites ofimáticas tradicionales: Gmail (correo electrónico), Meet (herramienta de videoconferencia imprescindible para la interacción entre alumnado, profesorado y familias en caso de educación telemática), Calendar, Drive (almacenamiento en la nube) editor de textos “Google documentos”, hojas de cálculo, presentaciones etc. (,,,)”“El equipo directivo del centro educativo solo y únicamente debe dar de alta en este Servicio al alumnado si está en posesión del Documento de Consentimiento Informado de las familias que han firmado aceptando las condiciones de participación. Dicho documento deberá ser custodiado por el centro. “, figurando un link al “documento de consentimiento informado”.

El reclamante efectúa sobre el manual de acogida una serie de puntualizaciones, que pueden resumirse en:

a) *“Uso de la herramienta videoconferencia con padres, cuando sobre estos no existe actividad de tratamiento, parece se va a utilizar para “labores administrativas”, cuando se informó que es un recurso de apoyo que complementa la oferta de plataformas de la Consejería, pero no se aclara que el padre o alumno puede optar por las herramientas propias de la Consejería, “ya que solo se solicita autorización a la GSUITE”. “No se aclara la implicación de su rechazo”.*

b) *“Coexistencia de las cuentas de correo de dominio.es para el funcionamiento de GS educativo, con la institucional de la cuenta Gobierno Canarias org. Así se indica en las “PREGUNTAS FRECUENTES” de gobiernocanarias, a la que se accede a través de un link en el propio documento de “consentimiento informado”, ***URL.2, que, además, ofrece información sobre la aplicación. “La cuenta “***EMAIL.1” viene incluida y es necesaria para el acceso al paquete de los servicios de Gsuite. El correo corporativo a efectos oficiales sigue siendo “***EMAIL.1”.*

Entre otras cuestiones que se plantean en PREGUNTAS FRECUENTES, que merecen su mención, destacan:

- *“Si ya tenemos funcionando una cuenta de Google, con dominio de centro, ¿puedo seguir utilizándola?”*

En estos momentos, ya se ha puesto en marcha el servicio del G Suite Educativo de la Consejería de Educación, tras la firma del Convenio con Google para ofrecer cuentas de un G Suite de la Consejería de Educación al profesorado y alumnado de los centros educativos públicos de Canarias.

El uso de este G Suite Educativo corporativo ofrece la garantía de estar recogido en el convenio que ha firmado la Consejería de Educación, y para ello se ha creado el correspondiente registro de actividad de tratamiento (RAT) de datos personales denominado “solución tecnológica para la comunicación y la colaboración G SUITE”.

Por tanto, se recomienda utilizar el G Suite Educativo de la Consejería de Educación para estar amparado por el citado convenio y registrado en la actividad de tratamiento de datos especificada. Ya que el resto de G Suite distintos al de la Consejería, no estarían recogidos en dicho convenio, ni en el citado registro de tratamiento de datos.

Por último, hay que destacar que el dominio utilizado en el G Suite Educativo de la Consejería de Educación, "canariaseducación.es" es un dominio registrado y autorizado, atendiendo a la ORDEN de 23 de mayo de 2019, por la que se aprueba la política de dominios en internet de la Administración Pública de la Comunidad Autónoma de Canarias,

- "Para qué se puede usar el correo "***EMAIL.1"?"

El uso del correo electrónico del profesorado y del alumnado asociados al G Suite Educativo de la CEUCD solo se puede utilizar para fines educativos, siempre que los usuarios hayan firmado el consentimiento informado del uso de los servicios del G Suite.

Para finalidades administrativas, de gestión y de comunicación con las familias se utilizará el correo corporativo del centro y del profesorado "***EMAIL.1"

- "¿Es posible exportar toda la estructura del G Suite actual, propia del centro, a la nueva cuenta de G Suite de la Consejería de Educación?"

No, la estructura de un G Suite anterior no se puede migrar al G Suite Educativo de la Consejería de Educación, pero se puede transferir o copiar el contenido de algunos de los servicios del G Suite, tal y como se explica en el apartado correspondiente de esta página web."

- "Cuando se activó el servicio de G Suite del centro se le hizo firmar un consentimiento a las familias. ¿Sirve ese consentimiento para el G Suite Educativo de la Consejería? ¿Con qué frecuencia se pasa dicho modelo?"

Solo tiene validez el modelo de Consentimiento Informado realizado expreso para hacer uso del servicio del G Suite Educativo de la Consejería de Educación. Este documento firmado se custodiará en el centro y se solicitará a todo el alumnado para poder gestionar sus cuentas en el G Suite.

Cada alumno o alumna debe tener dicho documento firmado cuando se incorpore por primera vez al centro, y no será necesario volver a solicitarlo, a no ser que se quiera revocar.

"¿Qué ocurre cuando se transfiere el contenido de un G Suite cualquiera al nuevo G Suite Educativo de la Consejería de Educación?"

Los servicios que se transfieren a través de la "Gestión de la cuenta" del G Suite son el Gmail y el Drive. En este proceso, que lo tiene que realizar cada usuario, se transfieren todos los datos del correo electrónico de Gmail (excepto los contactos, los chats y las tareas) y los documentos de su propiedad que figuren en Google Drive (excepto los archivos de la sección «Google Fotos» de Drive y los archivos incluidos en unidades compartidas).

Los archivos originales permanecen en la cuenta del G Suite de origen, de manera que, una vez realizada la transferencia, los cambios que se hagan en los archivos copiados no afectarán a los originales; puesto que se transfiere la propiedad a la nueva cuenta de G Suite Educativo."

SEGUNDO: El reclamante alude a su reclamación no satisfecha de 20/06/2021, dirigida a la Viceconsejería, referida a hechos sucedidos en el IES en ese curso 20/21 y en el anterior 19/20. *“Solicita que se evalúen las infracciones que se han comunicado al DPD en materia de la LOPDGDD, realizando la resolución sancionadora.”*

Refiere el relato de los hechos en el EXPONE del documento *“Registro general electrónico del Gobierno de Canarias”* y señala cinco anexos que presentó en su momento frente al IES con los que están relacionados los hechos:

Anexo I- 8/07/2020 entrega de matrícula firmada al IES.

Anexo II- 7/11/2020, reclamación a IES, registro entrada 543. No se aporta copia del mismo

Anexo III- 3/12/2020 respuesta del IES, reg. salida 129, (no es tal, es un aplazamiento en la respuesta que se toma el reclamado)

Anexo IV- 28/12/2020 respuesta de IES.

Anexo V-Respuesta a escrito de IES de fecha 28/12/2020.

Inicia la reclamación:

1- *“Para el presente curso 20-21”, realizó “la matrícula por medios telemáticos en la Consejería”, además el IES requirió su presentación que se efectúa de forma presencial “el 8/07/2020”, indicando la no conformidad con el anexo incluido denominado: “SOLICITUD DE CUMPLIMIENTO DEL RGPD”. En relación con esa manifestación, el anexo 1 no es aportado y no se puede saber los términos en los que expresa su no conformidad.*

- *“Expresa el desacuerdo en el uso de herramientas ajenas a la Consejería, incumplimiento del RGPD a la hora de solicitar nuestra autorización para el alta de nuestro hijo en la aplicación GSUITE y MICOLEGIOAPP,” “expresando nuestra no conformidad.” - “Al comienzo del curso”, “sin autorización volvieron a dar de alta a nuestro hijo nuevamente en dicha plataforma, aun habiendo expresado nuestra no conformidad en la matrícula, incumpliendo lo solicitado en el anexo” No aporta copia del documento en el que se producen las manifestaciones que expresa*

2- Al *“final de curso pasado “al proporcionar a GOOGLE la edad real de nuestro hijo, esta cuenta fue bloqueada por GOOGLE indicando que no tenía edad suficiente 12 años, la edad mínima para tener una cuenta de gmail son 14 años.”*

3- *“Además, se produjeron nuevas faltas, por lo cual el 7/11/2020, se presentó un NUEVO escrito ante el IES-ANEXO II- entrada 543”, al decir nuevo, se desconoce cuál fue el anterior, si bien tampoco aporta este de 7/11/2020 “en el que “exponiendo su lista de reparos al uso de la aplicación, pidiendo la eliminación de usuario, eliminación de los correos en buzones de destino del alumno y del padre, con la exportación de la información generada al dar de alta en la plataforma. (Anexo II), añadiendo:*

3.1 *“No se aclara en la cláusula de consentimiento de forma correcta que no pueda interpretarse que la solicitud de autorización podría ser para menores, de uso de la plataforma empresarial GSUITE, apta esta para mayores de edad.”*

3.2 *“No se ha contestado a la negativa a su uso” “en los tiempos indicados en el anexo a la matrícula”.*

Alude al uso o consecuencias del mismo en las distintas aplicaciones de la plataforma GS:

3.3 *“Alta en la “plataforma cloud” sin consentimiento paterno, a través de un acuerdo firmado directamente por el Director con GOOGLE”.*

3.4 *“Uso para la formación de su hijo de correos ajenos a la Consejería, con transferencia internacional de datos, especialmente, tras la anulación del escudo de privacidad por sentencia de TJUE de 16/07/2020.”*

3.5 *“Uso de los mismos correos electrónicos para labores administrativas del centro, con el dominio del IES.es.”*

3.6 *“Uso de la herramienta videoconferencia de la plataforma GS para comunicación con padres y alumnos, sin autorización para su uso.”*

3.7 *“Uso de formularios de GOOGLE de forma indiscriminada y en cantidades desproporcionadas, sin que se aclare el motivo de la solicitud de dicha información, con datos excesivos, como por ejemplo los de educación física o, de tutora.”*

3.8 *“Proporcione una plataforma telemática para la formación, que esté “bajo el paraguas de la Consejería” que incluya el uso de cuentas corporativas del Gobierno de Canarias para la comunicación con padres o hijos tanto para la actividad lectiva como administrativa.”*

4-Aporta copia de respuesta del IES, Anexo 4, de 28/12/2020 (dice responder al de 27/11/2020, registro 543), exponiendo sobre los cinco puntos que solicita, que va a proceder *“en enero a ejecutar los puntos 1, 2 y 5 que encabezan su escrito. Alude a:*

4.1 *“El correo electrónico utilizado por el equipo directivo, el profesorado para comunicación interna y externa con los sectores de la comunidad educativa es el corporativo y autorizado en la programación general anual para este curso 2020 21”.*

4.2 Le informa de la suscripción de la Consejería un Convenio con GSUITE, publicado en el BOC de 19/10/2020, *“y por tanto, posterior a la utilización de la herramienta Google por parte del centro”*, estando la misma bajo las garantías de protección de datos establecidas ofreciendo dos links sobre el alcance y otros recursos de la actividad de tratamiento de espacios *virtuales de aprendizaje y colaboración-* orden de 25/05/2018, y otra orden de la Dirección General de Ordenación, Innovación y Calidad (DGOIC), de 11/09/2020, registra la actividad

de tratamiento de “solución tecnológica para la comunicación y la colaboración GSUITE”.

5) En ANEXO 5, presentó “respuesta al escrito del IES” el 29/01/2021 (aporta copia), indicando:

5.1 A pesar de comunicarse la existencia del acuerdo de la Consejería con Google “declinan su uso,” y como apreciaciones indica:

5.1.a “Espera que “la eliminación de la cuenta de la plataforma se realice en los términos solicitados”.

5.1. b “Los correos corporativos llevan al final .org y no es así, “ya que son bajo el contrato firmado entre el centro y GOOGLE y que no intervino la Consejería del mismo”.

5.1.c “Nos mostramos de acuerdo en el uso de otra plataforma telemática disponible, la EVAGD, y dispuestos a migrar la información a dicha plataforma”.

6) “No han recibido respuesta por parte del centro, observando “nuevas faltas” (se detallan en los puntos 6.1 a 6.4 del “Registro General electrónico del Gobierno de Canarias”, referidos al uso y la forma del mismo en las aplicaciones de la plataforma:

6.1- “Uso de formularios Google, por ejemplo, para realizar encuestas para realizar exámenes y trabajos, añadiendo más datos de carácter personal, las calificaciones de nuestro hijo después de haberles indicado que no autorizamos su uso el servicio. Google formularios no forma parte de GS Suite, siendo eso sí, una herramienta que pertenece a Google.

6.2- Uso de correos no corporativos. La comunicación con los profesores continúa siendo con correos denominados por ellos como corporativos, cuando no lo son, siendo los corporativos los finalizados en.org.

6.3- Acceso de menores a servicios como mayores de edad. Se trata de los servicios adicionales de GS como por ejemplo YouTube, Maps o bloggers sin restricción de edad, ya que al obtener el consentimiento los usuarios de GS para centros educativos, se utiliza para servicios adicionales autorizados, cuando ni siquiera se ha incluido YOUTUBE en el acuerdo que ha alcanzado la Consejería con Google, siendo servicios adicionales, con política de privacidad distinta al resto en las aplicaciones.

6.4 Desde el directorio de contactos de GS, se tiene acceso al listado completo de alumnos y profesores del centro incluyendo su nombre completo, correo electrónico y foto, pudiendo facilitar la filtración de los mismos fuera de la plataforma.”

7) Como continuación a la reclamación, aporta copia de escrito de la Viceconsejería de Educación Universidades y Deportes que responde a su reclamación de 20/06/2021, en e mail de ***FECHA.3, indicando:

Se ha enviado un documento desde el Área de Tecnología Educativa (DGOIC) al IES “de las orientaciones para el uso educativo, seguro y responsable de las tecnologías digitales, teniendo en cuenta la protección y privacidad de los datos.”

Certificado del IES de la “cancelación de la cuenta de correo electrónico de su hijo”, (dicho certificado se le adjunta como archivo a ese correo).

El IES “Para el curso 2021-2022, ya ha solicitado para su centro educativo el dominio “canariaseducación.es”, para estar dentro del G-Suite de la CEUCD, así como también las gestiones necesarias para poder dejar sin efecto el anterior “.

TERCERO: Presenta el reclamante ante esta AEPD un escrito de 14/12/2021, manifestando:

1 “En el momento de la presentación de esta reclamación ante la AEPD, no teníamos respuesta por parte del IES” que se produce el *****FECHA.2**, aportando su copia en ANEXO 6.

“Resaltamos que esta reclamación la hemos acotado a los dos cursos anteriores 2019-2020, 2020-2021 y la solicitud de matrícula del presente curso 2021-2022.”

“Durante el presente curso hemos presentado nuevas reclamaciones ante el DPD referidas a la plataforma GSuite educativa de la CEUCD que no tienen que ver con la GSuite propia del Centro IES La Laboral”, la cual es objeto de la actual reclamación.

2 En el ANEXO 6, que contiene la respuesta de la reclamada de *****FECHA.2**, “a los escritos presentados hasta la fecha de hoy”, cabe resaltar, junto a las observaciones del reclamante:

2.1 “El 16/01/2021 se procede a la (...) por parte del coordinador TIC (por protocolo se queda 20 días en suspenso hasta su eliminación total).”

“Se informará al equipo educativo de **XXXXXX**, que el alumno no podrá utilizar más la herramienta GSUITE, establecida como entorno virtual de aprendizaje tipo reflejado en la PGA del centro”.

Observación: “No entendemos con qué potestad realizan dicha eliminación, sin proporcionarnos nada de lo solicitado por escrito, sin ningún plan de migración y sin la copia del contenido de la cuenta.”

“El 18 de enero, el padre del alumno, solicita” en “conversación telefónica con el coordinador TIC, que se reactive la cuenta del dominio ieslalabraldelalaguna.es hasta que presente un nuevo escrito, al no estar de acuerdo con las acciones alternativas y proponer que se utilice entre otros, el entorno EVAGD (entorno virtual de aprendizaje alojado en los servidores de la Consejería de Educación, Cultura y Deportes (CEUCD) (no utilizado por la mayoría de los docentes de la ESO) y la app de videollamada JITSI. (...)

Observaciones: “Aclaremos que la propuesta del coordinador TIC consistía en:

“Migrar la cuenta de nuestro hijo de la GSuite propia del IES *****IES.1** a la GSuite Educativa de la CEUCD” *“para lo que se requiere un consentimiento informado, que no nos habían solicitado. Indicamos que con la experiencia que habíamos tenido en cursos anteriores, íbamos a rechazar su uso.”*

“Se le expresó que nuestra voluntad era que la migración se realizase a la plataforma principal y propia de la Consejería y que no eliminase la cuenta” *“estábamos preparando un escrito expresando nuestra voluntad de migrarlo a EVAGD”. “Dicho escrito se presenta por registro de entrada del centro el 29/01/21, sin obtener respuesta. Es más, nuestro hijo continuó utilizando la GSuite propia del centro y nunca se nos proporcionó nada de lo requerido en dicho escrito que incluía la copia de seguridad del perfil de nuestro hijo contenida en el Anexo 5, 29-01-21 Respuesta a escrito de IES La Laboral de fecha 28_12_2020.pdf. “*

2.2-“El 10/06/2021 se crea una cuenta de código acabado en 91@canariaseducación, atribuida al IES (orden de 23/05/2019, prueba política de dominios en internet en la APU de Canarias) y se articulan comunicaciones oficiales de procedimientos para el curso 21-22 con la comunidad educativa”, como los de 18/06 del Director, informando de su implementación como correo educativo corporativo del Gobierno de Canarias, y de la misma fecha, del coordinador TIC “a todo el alumnado, de información sobre eliminación de las cuentas del dominio ieslalaboraldelalaguna.es al finalizar el curso escolar 20/21”. También, el 24/06/2021, por “parte del del coordinador TIC se informó a todo el profesorado del IES de la eliminación de cuentas de dominio ieslalaboraldelalaguna.es al alumnado al finalizar el curso escolar 20/21 y la prohibición de comunicar con el correo del profesorado con alumnado y familias a partir del mes de julio” ... Se les informa cómo transferir los contenidos de la GS antigua a la nueva”.

“Tras haber finalizado el curso escolar 21-22” (indudablemente, se tiene que referir al curso 20/2021), “el 7/07, se realiza la eliminación definitiva de la cuenta del alumno **B.B.B.**...del dominio ieslalaboraldelalaguna.es, eliminación definitiva el 26 del mismo mes.”

Observación: “Se resalta que en el correo del responsable TIC indica que se realizarán a mediados de septiembre (se incluyen al final de este escrito los correos del responsable TIC para la eliminación de las cuentas) “, cita textualmente: “Una vez terminado el curso escolar, se recuerda que deben descargar todo el material del Drive y correos, pues a mediados de septiembre se procederá a la eliminación de las cuentas actuales de Gsuite, para asignar las nuevas del curso 2021/22. Durante el verano y principios de septiembre permanecerán activas para tareas de recuperación.” Aporta copia del citado correo del IES de 18/06/2021 a los alumnos y tutores, en el que se expresa en los citados términos.

“El pasado 9/09/2021, la familia del alumno no autoriza que utilice la G SUITE del alumnado en centros docentes de titularidad pública de la

Consejería de Educación, (denegación en el documento de solicitud de matrícula del formulario único y a través de consentimiento informado. “)

Añade captura de pantalla de la eliminación de la cuenta del hijo del reclamante del citado dominio y un certificado, que no se aprecia por no ser legible.

2.3“El 28 de junio se recibe escrito del reclamante adjuntando anexos exponiendo cláusula ilegal reiterada en el proceso de matriculación de la matrícula del curso 2021/2022.”

Observación: “Ya se ha incluido en esta reclamación “.

En el punto 2 del anexo 6, continua el IES: “Sobre la reclamación, reiterada en el proceso de matriculación, en este caso, de la del curso 21-22” en el proceso de matrícula mediante el documento unificado, no se exige ni es obligatorio adjuntar el anexo 1 del IES” en las indicaciones de matriculación descritas en la web del centro no se indica la obligatoriedad de la presentación del ANEXO”. Aporta una captura de pantalla, en la que informa:” descargar el anexo 1” que contiene cierta información sobre instrucciones para el pago, licencias digitales-no obligatorio-según instrucciones en el Anexo 1. “Hay que recordar que, si se realiza el pago en este procedimiento no obligatorio, entrará en la oferta que se le hace desde el centro, con un 50% de descuento en el precio respecto al que tendría que pagar si lo hace directamente a las empresas” y resalta la conveniencia de adjuntar todos los documentos descritos en los puntos anteriores -el anexo 1-.

Manifiesta el IES que “en el anexo 1 se describe, en el apartado de consentimiento informado, al adjuntar este documento como anexo a la solicitud de matrícula” sin obligar a su presentación, indicando que en el caso de presentarlo voluntariamente se entenderá consentimiento informado.”

“Los interesados en matricularse en el IES tienen la opción a no estar de acuerdo con el anexo 1 y no presentarlo, y sí especificar obligatoriamente en el documento unificado de matrícula el consentimiento o no en el apartado de medios de difusión, donde se le comunica:” consentimiento informado tratamiento de imágenes voz del alumnado en centros docentes de titularidad pública de la Consejería de Educación universidades cultura y deportes”.

“El anexo del IES para la matrícula del curso 21/22 no es más que una herramienta para mejorar la gestión interna del centro en la búsqueda de mejora continua y Calidad Educativa de carácter no obligatorio”.

Observación:” Resaltamos que el documento ANEXO 1 no permite rechazar de forma diferenciada cada uno de los apartados contenidos en el mismo.

“Destacamos que, junto a dicha cláusula, se incluye en el mismo anexo un descuento en el coste de los libros del 50% que está incluido en el mismo y no vemos cómo se puede disponer el descuento de los libros y además el rechazo de la cláusula ilegal ya que ambos están incluidos en el mismo anexo.”

“Por otro, no se entiende que hagan alusión al apartado de la matrícula “Medios de Difusión”, que es para la actividad de tratamiento de “Consentimiento informado tratamiento de imágenes voz del alumnado en centros docentes de titularidad pública de la Consejería de Educación, Universidades, Cultura y Deportes.” el cual no tiene que ver con la solicitud de consentimiento informado para la GSuite Educativa.”

2.4 En su punto 3, manifiesta el IES que *“Sobre la exigencia de recuperación de la información del perfil del usuario y de las copias de seguridad, se ha realizado el borrado de la cuenta de usuario tal como solicitaron, no pudiéndose recuperar tal información y habiéndose comunicado a todo el alumnado el 18 de junio que se iban a eliminar todas las cuentas, por lo que tuvo tiempo de haber realizado copia de seguridad de las mismas y de las copias de seguridad a la exigencia de recuperar la información del perfil del usuario.”*

2.5 Finaliza el IES en el punto 4, indicando que garantiza que recogida la no autorización para estar de alta en GSuite no se creará la cuenta y no podrá utilizarse. Ultima el escrito, aludiendo a las alternativas al trabajo del hijo del reclamante, como las entregas de tareas y a las licencias digitales, exponiendo opciones.

3- Como anexo 7, aporta el reclamante un e mail de la Viceconsejería, de 4/11/2021, dirigido a él, en el que le responde sobre uno anterior de *“la recuperación del perfil de usuario y copias de seguridad, al tratarse de un G Suite externo al que ofrece la CEUCD, solo puede realizarlo el propio centro, que tiene acceso a las mismas y la capacidad para gestionarlas. En todo caso, con carácter general es el propio usuario el que puede hacer copias de seguridad de sus cuentas. Deducimos que, o bien puede que se haya dado la circunstancia de que la cuenta se haya eliminado antes de que el usuario haya hecho una copia de la misma, o como aduce el interesado no disponía de permisos. La información existente en la red indica que las cuentas eliminadas permanecen durante 20 días:***URL.3”*. Transcribe que: *“El IES ***IES.1 responde que: “Ante la “exigencia” de la familia de “...la recuperación de la información del perfil de usuario de su hijo y de las copias de seguridad, que deberían de disponer el IES para corregir errores como los que ha cometido” informan que: Como indica el certificado del secretario del centro,(que ya se le adjuntó) se ha realizado el borrado de la cuenta del hijo de la familia, tal y como solicitaron, no pudiéndose recuperar la información, y habiéndose comunicado a todo el alumnado el 18 de junio que se iban a eliminar todas las cuentas “*

Añade que en la admisión a trámite se tenga en cuenta *“el uso de formularios por parte del Centro, y el uso de la aplicación MICOLEGIOAPP para comunicaciones con los padres y alumnos”*.

CUARTO: En el añadido del escrito del reclamante presentado en esta AEPD el 2/01/2022, reclama por el formulario de consentimiento de G SUITE que ha dispuesto la CEUCD, teniendo dos hijos estudiando en centros dependientes de dicha Consejería y habiendo presentado una previa reclamación el 12/10/2021 (aporta copia en Anexo 1 en modo resumen de 8 páginas, si bien no aporta la propia reclamación) por vulneración del ordenamiento jurídico en protección de datos, y se le ha respondido el 29/11/2021. Sigue con una introducción, resumen de los apartados incluidos en la reclamación, conteniendo hasta 13 puntos, conclusiones y solicitud. En el mismo escrito relata la respuesta de la Viceconsejería y sus observaciones.

No obstante, el resumen de lo presentado por el reclamante y la respuesta de la reclamada, con las observaciones del reclamante en el resumen, se puede comprender el objeto de la reclamación.

En la respuesta, la Viceconsejería indica:

1) Informa de la finalidad de la petición del consentimiento-menores de 14 años-, mayores, *“para proporcionarle una cuenta del G SUITE educativo de la CEUCD y administrarla para el acceso a los servicios principales de Google y a los servicios adicionales necesarios para ejercer la función educativa, y para informar del tratamiento “solución de servicios digitales y telemáticos para la comunicación y colaboración G SUITE del alumnado”.*

Como observación del reclamante, indica que el formulario detalla los servicios que se ofrecen, *“principales”, y “adicionales”, “no permitiendo elección de los mismos”,* teniendo en cuenta que los servicios *“adicionales”* tienen términos de uso específicos.

La reclamada justifica además la no necesidad del consentimiento para el tratamiento de datos en el ejercicio de la función educativa, señalando la Guía para centros educativos de la AEPD y la LO 2/2006, disp. adic 23.

Como observaciones del reclamante *“eso sería para el uso de herramientas propias donde no exista cesión de datos a terceros o no exista transferencia de datos internacional. Es más, no se hace para el caso de EVAGD o la App Alumnado y familia.” No exime a la CEUCD del deber de cumplir con el resto de los requerimientos de la RGPD/LOPDGDD, por ejemplo, la definición de la política de privacidad, actividades de tratamiento de datos, evaluación de impacto y realización de análisis de riesgo entre otros.”*

-Sobre lo contestado en *“política de seguridad”*, refiere el reclamante que la respuesta es sobre los servicios propios de la Consejería, que no tienen que ver con la herramienta GS educativa.

-Sobre el *“análisis de riesgos”*, señala el reclamante que alude a las acciones sobre el tratamiento de *“datos personales relativos a los espacios virtuales de aprendizaje y colaboración”*, explica la finalidad del mismo, observando el reclamante que este análisis es el de la actividad de o para los servicios propios de la CEUCD, denominándose de otro modo la de GS: *“Solución de servicios digitales y telemáticos para la comunicación y la colaboración G SUITE”.*

2) Sobre la *“Evaluación de impacto”* indica la reclamada que de G SUITE, se ha realizado con la herramienta *GESTIONA* puesta a disposición por la AEPD, *“que*

permite evaluar de manera anticipada cuales son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos”, arrojando un riesgo residual aceptable, mencionando diversos documentos anexos a la EIPD como el documento “gestión de riesgos GS”, “listado de cumplimiento normativo GS”. Además, califica como documentación crítica a efectos de conocimiento por terceros. Como observación, el reclamante indica que no figura la fecha en que se hizo y no se ha evaluado su cumplimiento.

3) En cuanto al formulario de obtención del consentimiento que aporta el reclamante a través de link, titulado:

“CONSENTIMIENTO INFORMADO DEL USO Y TRATAMIENTO: “SOLUCIÓN DE SERVICIOS DIGITALES Y TELEMÁTICOS PARA LA COMUNICACIÓN Y LA COLABORACIÓN G SUITE DEL ALUMNADO EN CENTROS DOCENTES DE TITULARIDAD PÚBLICA DE LA CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS

Manifiesta el reclamante sobre G SUITE educativa y el Convenio:

-Hay faltas en el deber de informar y en transparencia de la información y transparencia en el modelo del consentimiento, extensible a:

- *“Evaluación de aplicaciones en servicios principales y adicionales a nivel de rastreadores, ubicación de los servicios, cookies analíticas y política de privacidad”.*

- *“Ubicación de la información. Incumplimiento de la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18”, Schrems II.*

-*No se aplica el principio de minimización de datos.*

-*Incumplimientos en la definición de la actividad de tratamiento de datos.*

-*Como usuario para el acceso a GS educativa hace uso del identificador del CIAL, dato de carácter personal, Además, es utilizado como identificador para los correos que, aunque está restringido el envío de correos fuera de la plataforma se proporciona este dato de carácter personal a otros pudiendo utilizar un identificador anónimo, por ejemplo.”*

Considera en sus conclusiones que se está produciendo una violación del derecho fundamental a la intimidad.

QUINTO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), el 1/10/2021 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. Se le solicita en concreto:

“1. La decisión adoptada a propósito de esta reclamación.

2.En el supuesto de ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD, acreditación de la respuesta facilitada al reclamante.

3. Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

4. Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

5. Cualquier otra que considere relevante.”

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 1/10/2021 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

SEXTO: Con fecha 30/11/2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

SÉPTIMO: 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.

Se solicitó el 25/01/2022: “información relativa a utilización de la G Suite para Centros Educativos por parte del IES *****IES.1**”, en concreto:

1. “Descripción de los tratamientos de datos personales que se realizan con la citada información, indicando que datos son relativos a los alumnos y que datos son relativos a los padres o tutores.”

Con fecha 18/02/2022, a pesar de que indica que se recaba información del IES, se recibe respuesta de la reclamada en la que alude al servicio G SUITE educativo, no del IES, que se deduce de la reclamación del reclamante fue usado antes, sino del implantado a través de la suscripción del Convenio que hace la CEUCD con GOOGLE IRELAND. Manifiesta:

“El servicio de G Suite educativo de la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias solo trata datos del alumnado y del profesorado de centros educativos públicos no universitarios dependientes de dicha Consejería. En ningún caso trata datos de los responsables legales o familia del alumnado.

El alumnado accede a los servicios del G Suite Educativo con autenticación CAS (Sistema Centralizado de Autenticación)” y los datos que Google trata del mismo son:

Nombre
Apellidos
XXXX (...)
Correo (**EMAIL.1)
Avatar del alumnado

“Los servicios propios del G Suite (Google Workspace for Education Fundamentals) hacen uso de diversos datos académicos y profesionales proporcionados por los usuarios: producciones del alumnado, calificaciones, grupos, materias...”

La finalidad del tratamiento de estos datos es el acceso al servicio del G Suite Educativo con fines estrictamente educativos, para apoyar las enseñanzas de los centros docentes públicos no universitarios de Canarias.”

1. *“Base legal que soporta los tratamientos de datos realizados con la aplicación GSUITE. En caso de que se recabe el consentimiento de los tutores, copia de los consentimientos de los tutores legales del alumno del centro”.*

Manifiesta que: “La base jurídica sobre la que se desarrollan los tratamientos de datos personales realizados con la aplicación GSUITE viene conformada por los siguientes preceptos legales:

-El artículo 6.1.a) RGPD.

Además, este tratamiento se fundamenta en el cumplimiento de obligaciones legales y en el ejercicio de poderes públicos conferidos al responsable del tratamiento”.
Menciona:

-Artículos 83.1 y 92 de la (LOPDGDD) que reconoce el derecho a la educación digital, y el relativo a la protección de datos de los menores en internet.

- El artículo 2.1.i) de la Ley Orgánica 2/2006, de 3/05 de Educación, en la redacción dada por la disposición final 10ª de la LOPDGDD.

- El apartado 2 del artículo 111 bis (“Tecnologías de la Información y la Comunicación”) de la referida Ley Orgánica 2/2006, de 3/05, de Educación,

- El artículo 24 (“Espacios educativos virtuales y nuevos entornos para el aprendizaje y la comunicación”) de la Ley 6/2014, de 25/07, Canaria de Educación no Universitaria,

- Ley Orgánica 3/2020, de 29/12 por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación

- Plan de Acción de Educación Digital (2021-2027).

Se aprecia que el formulario de *“consentimiento informado”* se refiere al consentimiento informado como base jurídica que *“permitirá el tratamiento”*. Aporta copia en documento 2.

2. *“Información facilitada a los padres o tutores de los alumnos en relación con los tratamientos de datos personales que se realizan con la citada aplicación.”*

Manifiesta que: “Los padres o tutores del alumno no consienten el tratamiento “solución de servicios digitales y telemáticos para la comunicación y la colaboración G Suite”, por tanto, no se le ha creado perfil de usuario en el G Suite.

Aportan copia documento 1 del “No consentimiento de los padres o tutores” a través del “formulario de consentimiento informado” a los servicios G SUITE for EDUCATION”, fechado en 9/09/2021, incluidos en la actividad “solución de servicios digitales y telemáticos para la comunicación y la colaboración G SUITE”.

Manifiesta el reclamado que había expuesto en la página de la Consejería en la fecha de solicitud de matrícula del curso 2021-2022 el formulario de consentimiento informado.

3. “Contrato o contratos firmados con la entidad suministradora de la aplicación, indicando si dichos contratos han sido suscritos por IES *****IES.1** o por la Consejería de Educación, adendas de protección de datos si las hubiera.”

De nuevo no alude a lo preguntado sino al Convenio. Añadiendo que, en el mismo, las partes se comprometen a través de las cláusulas que integran los TÉRMINOS GENERALES y LOS ANEXOS de las ADENDAS- “Adenda de Tratamiento de Datos al acuerdo GSUITE y/o productos complementarios-a efectos de referencia”- cuya versión vigente al momento de la firma se incluye como referencia al Anexo 2 del convenio y que se halla publicada en el citado BO.

Manifiesta, además, que se suscribieron “las Cláusulas contractuales tipo con el convenio.” Adjunta documento 4 en el que se indica que cuando el exportador (responsable del tratamiento) de datos ejecute un contrato de G SUITE y acepte con clic en el botón serán efectivas las cláusulas-incluidos los apéndices 1 y 2).

“Además, la MEMORIA recoge la justificación del interés público atendido en el referido convenio.”, las 19.000 unidades de tabletas adquiridas por la Consejería que utilizan el sistema operativo Android, que requieren para su uso e instalación de aplicaciones la utilización de una cuenta de Google y que tiene por objeto establecer las condiciones de colaboración entre las partes para el uso de la solución G Suite for Education (los “Servicios”). Las Partes reconocen y aceptan que el uso de los Servicios está regulado por los siguientes acuerdos, que la Consejería acepta expresamente al firmar el presente Convenio:

- Los Términos de G Suite for Education que se incluyen como Anexo 1 (Términos de G Suite for Education) a este Convenio,
- La Adenda de Tratamiento de Datos, Anexo 2

En el Convenio firmado se establece, en el punto 10.2 *Transferencia de datos*, que: “Si el almacenamiento o el tratamiento de los Datos Personales del Cliente implica transferencias de Datos Personales del Cliente desde el EEE, Suiza o Reino Unido a algún tercer país que no garantice un nivel de protección adecuado bajo la Ley Europea de Protección de Datos, y aplica la Ley Europea de Protección de Datos a las transferencias de dichos datos”, se detallan distintos escenarios en función de que el cliente haya suscrito dichas CCT, que puede hacer “a través de la Consola de Administración”.

El Convenio define:

Para conocer los servicios suscritos, dentro de la “solución tecnológica G SUITE for education, formada por un paquete de herramientas diseñado para permitir que los y las docentes y el alumnado accedan a un conjunto de servicios digitales y telemáticos orientados a mejorar el desarrollo de la actividad educativa y para que innoven y aprendan juntos”, se remite al punto 16 del ANEXO 1 “términos de G SUITE for education”, indicando “Servicios” significa los Servicios de G Suite para Educación prestados por Google y usados por el Cliente conforme al Acuerdo. Los Servicios se describen en: *****URL.4**, o en cualquier otra URL que Google pueda proporcionar”. Pinchando el link, lleva a una página de GOOGLE en la que informa en resumen de los servicios, sobre G SUITE, ahora GOOGLE WORKSPACE, en un apartado específico figura “for education”, se mencionan los servicios “Fundamentals”, versión gratuita, diferenciándolas de otras versiones. Señala que los “productos adicionales no están cubiertos bajo el acuerdo de GOOGLE WORKSPACE y no son servicios de este, sujeto a términos adicionales del producto.” Se indica que “comprende los servicios de Google Workspace Services excepto Client-Side Encryption, Currents, Google Cloud Search, Google Workspace Migrate, y Workspace Add-Ons. Esta edición también incluye: “Assignments, Classroom y Chrome Sync como servicios principales” Detalla en que consiste cada uno.

-“Assignments” es una aplicación para sistemas de gestión de aprendizaje que permiten a los usuarios finales distribuir, recopilar y calificar el trabajo de los estudiantes.

-“Classroom” es un servicio basado en la web que permite a los usuarios finales crear y participar en grupos de clase. Con Classroom los estudiantes pueden ver tareas enviar tareas y recibir calificaciones de los maestros.

-“Chrome Sync” es una función que permite a los usuarios finales sincronizar marcadores, historial, contraseñas y otras configuraciones en todos los dispositivos en los que iniciaron sesión en Chrome.”

Por lo demás, los servicios Google Workspace Services, a los que conviene remitirse para conocer cuáles son, pueden verse en esa misma página informativa.

“Consola de Administración” significa la herramienta online que Google facilita al Cliente a efectos de la comunicación o reporting de cierta información y la realización de otras funciones de gestión”

“Productos Adicionales”: productos, servicios y aplicaciones que no forman parte de los Servicios, pero a los cuales se puede acceder a través de la Consola de Administración, o de otra forma, para utilizar junto con los Servicios.”

1. “El carácter de la aplicación, indicando si es voluntaria o no. Fecha de implantación en el centro IES *****IES.1**, indicando quien autorizó ese uso originario al centro.”

Manifiesta que la CEUCD ofrece al profesorado y alumnado servicios virtuales, con la intención de proporcionar espacios para facilitar la combinación de la educación

presencial y digital de todos los centros públicos no universitarios de Canarias, y con el fin de garantizar la Ley Canaria de Educación no Universitaria y el logro de los objetivos del Plan de Acción de Educación Digital (2021-2027). Detalla los distintos entornos que ofrece de aulas virtuales y servicios digitales.

“Todas estas alternativas, cuyo uso no es obligatorio”, están disponibles para los centros públicos docentes no universitarios de Canarias, y se ofrecen con el fin de dar respuesta a las necesidades educativas, tanto del profesorado como del alumnado.”

“Los distintos espacios virtuales están amparados en la actividad de tratamiento de datos personales: “Espacios virtuales de aprendizaje y colaboración”, registrada mediante Orden de 25/05/2018, de la CEUCD.

En relación al carácter voluntario de G Suite, en el Expone III del Convenio entre la Consejería de Educación, Universidades, Cultura y Deportes y Google Ireland Limited, se señala que el uso de G Suite for Education en los centros docentes públicos dependientes de su Comunidad Autónoma no supone exclusividad del uso de este tipo de servicios digitales y telemáticos frente a otros similares.

En definitiva, en el uso de la aplicación G suite, nunca y bajo ninguna circunstancia se debe dar de alta al alumnado en el Servicio, por parte del centro educativo, sin que tenga firmado el documento de consentimiento informado de las familias.”

En cuanto a la fecha de implantación en el centro IES “*****IES.1**”, según la información recabada del IES, la aplicación G Suite para centros educativos se implanta en dicho centro educativo (...), “solicitándose el alta de los correos del alumnado por parte del equipo directivo, una vez se da el consentimiento informado firmado por los tutores legales.”

2. *“Copia del RAT donde se refleja la utilización de esta aplicación GSUITE.”*

Mediante Resolución de la Dirección General de Ordenación, Innovación y Calidad, de fecha 11/09/2020, se registró la actividad de tratamiento de datos personales relativos a la *“solución de servicios digitales y telemáticos para la comunicación y la colaboración G Suite”*.

Por otra parte, en virtud de Orden departamental n.º 185/2018, de 25/05 la Consejería tiene declarado el tratamiento “Espacios virtuales de aprendizaje y colaboración”.

Esa información figura en la web de gobiernodecanarias.

Se aporta como documento 6, el RAT de *“solución de servicios digitales y telemáticos para la comunicación y la colaboración G SUITE, figurando como base jurídica, el artículo 6.1. a).* En el apartado *cesiones de datos*, figura que no se prevé la cesión de datos. En el apartado *transferencias internacionales* *“se autoriza a GOOGLE IRELAND LIMITED mediante Convenio con la Consejería”*. En medidas de seguridad se alude a las del ENS.

“CATEGORÍAS DE DATOS PERSONALES Estructura:

- *Datos de carácter identificativos: Identificador (usuario corporativo o CIAL), nombre, apellidos, DNI, imagen, voz y otros datos identificativos como: el correo electrónico, usuario de redes sociales, firma, firma electrónica y cualquier otro sistema de firma y de identificación admitidos por las administraciones públicas.*

- *Datos de características personales: edad y sexo.*

- *Datos académicos y profesionales: centro educativo, enseñanza, nivel, área, formación, titulaciones, datos académicos, calificaciones y producciones del alumnado en cualquier tipo de formato.”*

El tratamiento denominado “espacios virtuales de aprendizaje y colaboración”, entre otros, fue objeto de registro de tratamiento, por una resolución de la Consejera de 25/05/2018, según figura en la copia del documento 7.

3. “Análisis de riesgos sobre los datos personales con el uso de esta aplicación”.

Manifiesta que la CEUCD ha realizado una Evaluación de Impacto en la Protección de Datos (en adelante, EIPD) de G Suite en la que participaron el responsable del tratamiento (Dirección de Ordenación, Innovación y Calidad), así como los Delegados de Protección de Datos de la Consejería.

“La EIPD consta de los siguientes documentos, que se adjuntan:

- DOCUMENTO 8 (página 74/128): “Informe de Evaluación de Impacto en la Protección de Datos” (EIPD) del tratamiento de datos personales “solución tecnológica para la comunicación y la colaboración GS”, de ***FECHA.1(...). Indica que ha usado la herramienta GESTIONA EIPD y la “Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD” publicada por la AEPD (de acuerdo con la web, fue publicada el 17/01/2018), debiendo señalarse que existe una guía publicada en junio 2021, titulada “gestión del riesgo y evaluación de impacto en tratamiento de datos personales”.

“Se ha llevado a cabo la EIPD, “dado que el mencionado tratamiento implica el tratamiento de datos personales de menores de 14 años, así como el uso de datos a gran escala”, y “el uso de nuevas tecnologías”.

- “Las principales categorías de datos objeto del mencionado tratamiento son datos de carácter identificativo, datos de características personales y datos académicos y profesionales.”, figurando más específicamente:

Estructura:

- *Datos de carácter identificativos: Identificador (usuario corporativo o CIAL), nombre, apellidos, DNI, imagen, voz y otros datos identificativos como: el correo electrónico, usuario de redes sociales, firma, firma electrónica y cualquier otro sistema de firma y de identificación admitidos por las administraciones públicas.*

- *Datos de características personales: edad y sexo.*

- Datos académicos y profesionales: centro educativo, enseñanza, nivel, área, formación, titulaciones, datos académicos, calificaciones y producciones del alumnado en cualquier tipo de formato.

Luego tiene otro apartado denominado “análisis del tratamiento”, en que se refiere a una mención breve a:

- ciclo de vida de los datos,
- actividades del proceso en el que se incluye el traspaso de datos de la persona en “DRIVE” o “deshabilitación de las cuentas de usuario: las personas borrarán sus datos. Al vencimiento del periodo de vigencia del convenio, la CEUCD dará instrucciones a GOOGLE para que elimine los datos”
- datos tratados, se indica entre otros, edad, imagen, calificaciones.
- tecnologías intervinientes se alude a “servicios del G SUITE”

Dentro de “análisis de la obligación de realizar una EIPD” se incluye “evaluación del nivel de riesgo, sin figurar una previa inclusión de “identificación de riesgos”. En evaluación del nivel de riesgo figuran:

1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender
2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento
3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos
4. Tratar datos personales con una finalidad distinta para la cual fueron recabados
5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización
6. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente
7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado
8. No tramitar o dificultar el ejercicio de los derechos de los interesados
9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma
10. Seleccionar o mantener una relación con un encargado de tratamiento sin disponer de las garantías adecuadas
11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento
12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad
13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable
14. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la seguridad en la organización
15. Error en la configuración de un sistema, aplicación, estación de trabajo, impresora o componente de red
17. Errores humanos en tareas de mantenimiento
18. Software malicioso (virus, troyanos, secuestradores de información)
19. Fugas de información

- 20. Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información
- 21. Robo o extravío de equipos, soportes o dispositivos con datos personales
- 22. Violaciones de la confidencialidad de los datos personales por parte de los empleados o personal externo de la organización
- 23. Disociación deficiente o reversible que permita la re-identificación de datos
- 25. Acceso a una información, servicios, aplicaciones o dispositivos de forma no consentida, por personas no autorizadas, traspasando de barreras (Hacking)
- 26. Manipulación o modificación no autorizada de la información
- 27. Incapacidad para asegurar la disponibilidad de la información
- 28. Ataque de Denegación de Servicio
- 29. Existencia de errores técnicos o fallos que ocasionen una indisponibilidad de los sistemas de información
- 31. Catástrofes naturales que afectan a las infraestructuras (inundaciones, huracanes, terremotos, etc.)”

Seguidamente se analizan las “medidas para la reducción del riesgo”, en un cuadro, indicando medidas, y en otra casilla: probabilidad/impacto/riesgo residual. (P//RR)

Sobre cada una de los 31” amenazas-riesgos” mencionados en el listado, destaca:

- “Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado”, “medida”: “realización de transferencias a países con garantías adecuadas. Realización de transferencias amparándose a garantías adecuadas. Realización de transferencias amparándose en alguna de las excepciones. Monitorización y revisión de proveedores” con P//RR “máxima”, “limitado”, residual Medio.

- “carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado el tratamiento”. Medidas: “identificación de los encargados de tratamiento partícipes de las actividades asociadas al tratamiento. Monitorización y revisión de proveedores. Supervisión y revisión de los servicios prestados por terceros. Comprobación del cumplimiento” P//RR: Despreciada/limitada/bajo”.

- “Tratar datos personales con una finalidad distinta para la cual fueron recabados”, medida: “identificación de la finalidad del tratamiento. Descripción de ciclo de vida del dato asociado a un tratamiento”, P//RR: Limitada/limitada/bajo.

- En: “Robo o extravío de equipos, soportes o dispositivos con datos personales”, P: Significativa /I: Limitada /RR Medio.

-Software malicioso virus troyanos secuestradores de información. Medidas. Valoración de eventos de seguridad a la información y toma de decisiones. Respuesta a los incidentes de seguridad. Notificación de los eventos de seguridad a la autoridad de control competente e interesados puntos recopilación de evidencias”, con P//RR “Limitada/ limitada/ bajo.”

- En *Fugas de información*, “medidas: valoración de eventos de seguridad de la información y toma de decisiones. Respuesta a los incidentes de seguridad. Notificación de los eventos de seguridad la autoridad competente e interesados. Recopilación de evidencias. P/IRR: Limitada, Significativa, medio.

Las mismas medidas aplica al “robo o extravío de equipos, soportes o dispositivos con datos personales” y al “hacking”

En cumplimiento, se indica: “En el documento de consentimiento informado se describen los servicios principales y servicios adicionales disponibles en función del usuario final, teniendo en cuenta las restricciones de edad de cada servicio para el cumplimiento normativo”.

“Analizada las fases del procedimiento se concluye que:

- los datos personales que la CEUCD facilita a Google son mínimos y por tanto constituyen un riesgo bajo.”

“MEDIDAS DE SEGURIDAD

Son aplicables las medidas de seguridad de acuerdo al Anexo II (Medidas de seguridad) del Real Decreto 3/2010 de 8/01, por el que se regula el Esquema Nacional de seguridad en el ámbito de la Administración Electrónica”. Añade que se define en el apartado dos del anexo 1 del convenio con GOOGLE, que dispone como encargado, “de certificado de conformidad con el ENS” EIPD con categoría alta”.

Igualmente, refiere en “almacenamiento” “GOOGLE Drive” y en el de “tecnologías intervinientes:” DRIVE”. En el apartado de “cesión o transferencia de los datos a un tercero para su tratamiento”, figura sin ninguna referencia.

También indica en “optimización del tratamiento”, que:

“Tanto alumnado como profesorado acceden a su cuenta de Gsuite a través de pasarela CAS (Servicio de autenticación centralizada) con usuario y contraseña corporativos del Gobierno de Canarias, que en ningún caso es accesible por Google”.

El resultado es de “riesgo residual aceptable”.

Al documento de EIPD se le anexan:

Anexo 2: GESTIONA EIPD GSUITE, documento resultante de la herramienta GESTIONA EIPD. Figura como documento 9. Consiste en unos cuadros en el que figura separado por secciones una pregunta una respuesta y una justificación. Existen las siguientes secciones:

1- “análisis de la necesidad de realizar una EIPD”, destaca en el apartado 5, tecnologías empleadas para el tratamiento: ¿se prevé el uso de tecnologías que se pueden percibir como inmaduras como de reciente creación o salida al mercado o con elevado riesgo para el acceso no autorizado? respuesta no, justificación:” la tecnología empleada cuenta con certificado del esquema Nacional de Seguridad en nivel alto”.

En el apartado de encargados de tratamiento, se indican respecto a las transferencias, que se prevé la transferencia de datos a Google mediante convenio.

-Ciclo de vida a los datos

2- *“análisis de la necesidad y proporcionalidad del tratamiento”*.

3- *“3 y 4 identificación de riesgos”*

En su apartado de *“1. Amenazas y riesgos”*, se reproducen los 31 señalados arriba, más el de *“Deficiencias en los protocolos de almacenamiento de los datos personales en formato Físico”*

3- *“5 Gestión de riesgos”*, cuadro ya mencionado arriba en el que, de las 31 amenazas, se indican las medidas y la P/I/RR.

Anexo 4: Listado de cumplimiento normativo GSUITE, documento para identificar los requisitos de cumplimiento del RGPD, documento 11.

-En los años 2018 y 2019, se llevó a cabo un análisis de riesgos de todos los tratamientos de datos personales gestionados por este Departamento, en el que se incluyó la *“actividad de tratamiento de datos personales relativa a los espacios virtuales de aprendizaje y colaboración”*.

Aporta:

-documento 12, resolución de 19/11/2018, de aprobación del gasto, y documento 13, titulado: *“informe de análisis de riesgos sobre las actividades de tratamiento de datos personales”* de la CEUCD, versión 1 de 5/12/2018, última actualización 7/05/2019. Se refiere a la implantación del ENS.

Relacionado con lo anterior, aporta el *documento 14: “plan de mejora de seguridad de la información”*, de 14/10/2019, para el sistema en general, sin especificar la solución GSUITE.

1. En la cuestión de: *“Medidas adoptadas para garantizar la integridad y confidencialidad de los datos personales de la aplicación.”*, manifiesta:

“La administración del G Suite Educativo la gestiona el personal del Centro de Atención al Usuario (CAU) de la Consejería de Educación del Gobierno de Canarias.

Los datos personales de la persona usuaria (nombre, apellido, CIAL y correo electrónico) se gestionan de forma centralizada desde “PINCEL EKADE” (Programa Informático para la gestión de Centros Educativos propio de la CEUCD).

La persona usuaria accede a los datos proporcionados en los distintos servicios con identificador y contraseña únicos.

El alumnado puede modificar su contraseña a través del servicio web de recuperación de contraseñas proporcionado por CAU_CE.”

En relación con las medidas adoptadas, se informa lo siguiente:

-La solución *GOOGLE CLASSROOM*, cumple con las exigencias del ENS.

-Los sistemas de información de Google, LCC, han sido todos ellos certificados con categoría ALTA, conforme con las exigencias del ENS, según se indica en el Informe de Auditoría del ENS, de fecha 14/10/2021. Aporta:

- documento 19, certificado de conformidad ENS GOOGLE SUITE Services de 16/10/2019, fecha renovación límite 16/10/2021, con el sello de ENAC. Los servicios que se incluyen y mencionan son entre otros CLASSROOM, Gmail, DRIVE, DOCS, FORMS, y se certifica que los sistemas de información reseñados, todos ellos de categoría ALTA, y los servicios que se relacionan han sido auditados y conformes.

-documento 20, de fecha 30/06/2020, de Centro Criptológico Nacional, sobre la aplicación *GOOGLE CLASSROOM*, *“que forma parte de GS for Education”*. Indica que *GOOGLE* expone en su web que tiene la conformidad para el ENS, que *“establece los principios y requisitos para una protección adecuada de la información en la Administración Pública española. Google Cloud (Google Cloud Platform y Google Workspace) ha acreditado su cumplimiento con los requisitos definidos en el ENS para los sistemas de información de categoría alta. “*

“Adicionalmente, y dentro del acuerdo en materia de protección de datos de países terceros con la Unión Europea, debe entenderse la necesidad de cumplimiento de los requisitos regulados a través del Reglamento Europeo 2016/679 (RGPD) que en su artículo 45, establece la continuación de los acuerdos suscritos en el año 1995 entre Europa y Estados Unidos para la protección de datos personales y que actualmente se supervisan a través de programa “EU-U.S. Privacy Shield”. Los servicios ofrecidos por la empresa Google, se circunscriben a este programa con una certificación obtenida en septiembre del año 2016 y que tiene como fecha de próxima revisión de certificación septiembre de 2020, tal y como establece el requisito de 4 años de revisión.”

- documento 21: *“Con fecha 18/10/2021, BDO Auditores S.L.P. certifica con el sello ENAC que ha auditado y encontrado conforme a las exigencias que regulan el ENS en el ámbito de la admón. electrónica, los sistemas de información que soportan los servicios de GOOGLE WORKSPACE, todos ellos de categoría ALTA, y los servicios que se relacionan incluidos en el anexo, y que se prestan desde los centros de GOOGLE localizados en Europa, encontrándolos todos ellos conforme con la norma que regula el ENS”*. Incluye un elevado número de servicios en el listado de servicios de GOOGLE WORKSPACE.

-documento 22 de 17/02/2022: *“Informe sobre el estado de la política de seguridad de la información de la (CEUCD)”*, en el que se alude a la realización de un informe de análisis de riesgos.

OCTAVO: Con fecha 13/09/2022, se acordó por la Directora de la AEPD:

“INICIAR PROCEDIMIENTO SANCIONADOR a **CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS-CEUCD**, con NIF S3511001D, por las presuntas infracciones de los siguientes artículos:

-dos infracciones del artículo 32 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, y a efectos de prescripción en el artículo 73.f) de la LOPDGDD

-una infracción del artículo 6.1 del RGPD, de conformidad con el artículo 83.5.a) del RGPD, y a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD.

-una infracción del artículo 13 del RGPD, de conformidad con el artículo 83.5.b) del RGPD, y a efectos de prescripción en el artículo 74.a) de la LOPDGDD.”

“a los efectos previstos en el art. 64.2 b) de la LPACAP, la sanción que pudiera corresponder sería de apercibimiento por cada una de las infracciones, sin perjuicio de lo que resulte de la instrucción.”

NOVENO: Con fecha 29/09/2022, se reciben alegaciones de la reclamada en las que:

- Reitera las manifestaciones realizadas el 18/02/2022

-En la información se ha seguido la opción de presentar una información básica en el momento de la recogida de la información, con remisión a información adicional, la segunda capara remite al “registro de actividades de tratamiento”, la publicación de la resolución de la DGOIC de 11/09/2020, por la que se registra la actividad del tratamiento “solución de servicios digitales y telemáticos para la comunicación y la colaboración G SUITE”, “donde se incluye la información sobre transferencias internacionales”, vuelve a indicar el link

*****URL.5** que lleva a una página de la web de la Consejería de Administraciones Públicas Justicia y Seguridad del Gobierno de Canarias, donde figuran las distintas unidades que gestionan actividades de tratamiento figurando en la CEUCD, entre otras, la citada Dirección General de Ordenación Innovación y Calidad y haciendo clic, figura en los registros de tratamiento de ese centro la “solución de servicios digitales y telemáticos para comunicación y colaboración G SUITE”, haciendo clic en ella se muestra la resolución integra de la D. Gral. de Ordenación, Innovación y Calidad, de 26/09/2022.

Estima que se informa del contenido básico a los interesados. Además, señala que tras el acuerdo de inicio se ha ACTUALIZADO la “actividad de tratamiento que se publica en el RAT”, aportando documento 6 A, pdf 2, en el que no figura la fecha de modificación. En el mismo, se contienen los datos de contacto de los DPD, se amplía la base jurídica añadiéndose la 6.1.c) y la 6.1.e) del RGPD y se suma la mención de los artículos 83 de la LOPDGDD, 2.1.i) de la LO 2/2006 de 3/05 de educación y el 24 de la Ley 6/2014 de 25/07 Canaria de educación no universitaria. En transferencias sigue sin variación: “transferencias internacionales: Se prevé la transferencia de datos. Se autoriza a Google Ireland Limited mediante convenio con la CEUCD, con domicilio social en Gordon House, Barrow Street, Dublín 4, Irlanda”

A raíz de la apertura de este expediente, han actualizado la información de la primera capa, incluyendo:

- información sobre las transferencias internacionales,
- posibilidad de presentar reclamación a la AEPD,
- inclusión sobre la información de los DPD y enlace directo a la resolución del registro de la actividad del tratamiento.

Aportan documento 2A, pdf 1, pág. 8, en la que se aprecia que no se contienen los datos de contacto del responsable, se han añadido las bases de legitimación referidas en el RAT actualizado, con el mismo contenido en “*transferencias internacionales*” que en el RAT completando los datos de contacto de los DPD y un apartado de “*derecho a reclamar ante la autoridad de control*”, faltando la referencia al artículo 13.2 c) del RGPD: “*cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;*”. En información adicional como segunda capa, figuran dos links que llevan al Registro de actividad de tratamiento.

Añaden que: “*al interesado, cuando se le ha informado directamente, se le ha indicado expresamente la posibilidad de reclamar ante la AEPD*”.

Aporta documento 2B, con e mail al reclamante de la Consejería al interesado de 28/04/2021 mencionando esa posibilidad y dando los datos de contacto de la DPD y varios desde la DPD al reclamante, como los de 19/07 y 5/10/2021.

Aporta documento 3C en el que se contiene la política de privacidad actualizada.

-En cuanto al Convenio con GS, señala y remite al link de diversas Comunidades autónomas que disponen del mismo Convenio con GS (Madrid, Andalucía y País Vasco). Aporta dictamen de la Agencia Vasca (pdf1 documento 4A) relativo al convenio de colaboración entre la administración general de la CAPV y GOOGLE COMMERCE LTD. para la utilización de los servicios “*GOOGLE WORKSPACE FOR EDUCATION*” en los centros docentes del Departamento de Educación, de 16/09/2021, en el que se indica que las cláusulas contractuales tipo (“*model contract clauses*” o “*standard contractual clauses SCC*”, complementan los “*términos del servicio*”, y la “*adenda de tratamiento de datos*” que fueron examinados a propuesta de la autoridad de protección de datos irlandesa por el Grupo de trabajo del artículo 29 que determinó el 30/12/2016 que si cumplían con los requisitos de la Decisión 2010/87 UE. El dictamen indica que las SCC se encuentran disponibles en una URL de GOOGLE y se corresponden con el texto de las SCC de la Decisión 2010/87/UE. Refiere la resolución TI/153/2017 de la AEPD que consideró adecuadas las garantías establecidas en los modelos de contratos aportados por GOOGLE INc y que GS obtuvo en 14/10/2019 el certificado de conformidad con el ENS.

Estima que las cláusulas contractuales tipo que se suscribieron junto al Convenio, aporta documento 4, reguladas en el artículo 46.2 del RGPD son garantías adecuadas para la transferencia de datos a terceros países, con validez confirmada por el TJUE en la citada sentencia, Schrems II.

Adjunta memoria del Convenio en documento 5, de 11/08/2020.

-Detalla todos los servicios virtuales que ofrece la CEUCD, alojados en servidores de su titularidad, excepto el de GS, que está en la nube, en combinación con la educación presencial y digital de todos los centros públicos no universitarios. Todos ellos no son de uso obligatorio. Estos espacios virtuales están amparados en la actividad de tratamiento de datos Personales: *“Espacios virtuales de aprendizaje y colaboración”*, mediante Orden n.º 185, de 25/05/2018, de la CEUCD en la que se agrupan todos los tratamientos de *“aprendizaje y colaboración que se usan en la Consejería”*.

Sobre estos tratamientos, se realizaron análisis de riesgos en el año 2019, aporta documentos 13 *“Informe de análisis de riesgos”* 14 *“Plan de mejora de seguridad de la información”* y 15, *“Orden de 21/05/2019 por la que se aprueba la política de seguridad de información de la CEUCD en el ámbito de la administración electrónica”*, todas en pdf, *“por lo que se partía de análisis de riesgos sobre el uso de espacios virtuales”*.

El documento 13, se comienza el 5/12/2018, actualizado a 7/05/2019, *“En el mismo, se detallan las actividades de análisis de riesgos llevadas a cabo y se presentan los resultados y objetivos previstos con la implantación de las medidas mínimas requeridas por el Esquema Nacional de Seguridad (ENS), permitiendo dar cumplimiento a lo previsto en el Reglamento General de Protección de Datos (RGPD) en lo referente a la evaluación de riesgos para el tratamiento de datos personales.” “Se han incluido los activos bajo responsabilidad de la CEUCD sujetos al cumplimiento del ENS”*.

El documento 14, primera versión 7/12/2018, actualizado 14/10/2019 tiene por objeto *“identifica las tareas a llevar a cabo para cumplir con los requisitos del Esquema Nacional de Seguridad para los sistemas de información de la Consejería de Educación y Universidades del Gobierno de Canarias, en adelante CEUCD.*

-La CEUCD *“ha realizado una EIPD de G SUITE usando la herramienta GESTIONA EIDP puesta a disposición por la AEPD.”* Indica que en los documentos 8 a 11 del pdf 3, se contiene la EIPD del tratamiento *“solución tecnológica para la comunicación y la colaboración GSUITE”*. Determina que *“Las principales categorías de datos objeto del mencionado tratamiento son datos de carácter identificativo, datos de características personales y datos académicos y Profesionales, y “dado que el mencionado tratamiento implica el tratamiento de datos personales de menores de 14 años, así como el uso de datos a gran escala”*. La EIPD se realiza entre el 8/03 y el 12/04/2021, considerando que se implanta en los colegios al inicio del curso 21/22, inicio septiembre 21. En base jurídica figura el artículo 6.1 a) del RGPD y el artículo 92 de la LOPDGDD.

A partir del RD 311/2022 de 3/05 por el que se regula el ENS van a realizare un análisis de riesgos de todos los tratamientos del departamento y de evaluación de impacto en todos los que proceda, conforme a lo recogido en el Pliego de Prescripciones técnicas para la contratación del servicio de “Consultoría y soporte para la adecuación al Esquema Nacional de Seguridad de la Consejería de Educación, Universidades, Cultura y Deportes”, en el que en su punto 3.1.4, dedicado al Análisis de riesgos y evaluación de impacto, se incluye expresamente el análisis de riesgos y la evaluación de impacto de los entornos digitales, o espacios virtuales, de

uso educativo que ofrece la Consejería a los centros públicos educativos y que implican el tratamiento de datos personales. Aporta documentos 23 a 26.

-Sobre las medidas de seguridad, se realizaron análisis de riesgos de todos los tratamientos del departamento en el año 2019, incluido el de “*espacios virtuales de aprendizaje y colaboración*”.

En el Convenio firmado, en el apéndice 2, figuraban las medidas de seguridad y GOOGLE informa de las medidas de seguridad para las transferencias internacionales (link) y en la Adenda suscrita figuraban medidas de seguridad aceptadas por la CEUCD.

DÉCIMO: Con fecha 19/05/2023, se emite propuesta de resolución, del literal:

“PRIMERO: Que por la Directora de la Agencia Española de Protección de Datos se sancione con multas de apercibimiento a CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS, con NIF S3511001D, por las infracciones de los siguientes artículos del RGPD,

- dos del 32 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, y a efectos de prescripción como grave en el artículo 73. f) de la LOPDGDD,

- 13, de conformidad con el artículo 83.5.b), del RGPD, y a efectos de prescripción como leve en el artículo 74.a) de la LOPDGDD.

- 6.1, de conformidad con el artículo 83.5 a) del RGPD, y a efectos de prescripción como muy grave en el artículo 72.1.b) de la LOPDGDD. multa de [Introduzca el texto correspondiente a

SEGUNDO: Que por la Directora de la Agencia Española de Protección de Datos se ordene a CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS, con NIF S3511001D, que en virtud del artículo 58.2.d) del RGPD, en el plazo de un mes, acredite haber procedido al cumplimiento de completar la información que debe contener según el artículo 13 del RGPD, y complete el análisis de riesgos de GS.”

La propuesta fue notificada el 22/05/2023, y con fecha 6/06/2023 se reciben las siguientes alegaciones:

1) Se ha modificado con fecha 6/06/2023 el RAT “*Solución de servicios digitales y telemáticos para la comunicación y la colaboración G Suite*” con fecha 6/06/2023. Adjunta link y documento 2 en el que se pueden ver entre otros, los datos del responsable del tratamiento y dirección y contacto, de los DPD y contacto y link, encargado de tratamiento a través de la suscripción del Convenio y en transferencias internacionales se añade que están sujetas a cláusulas contractuales tipo con un link.

2) Se ha actualizado y publicado el modelo de consentimiento informado, conforme a los aspectos señalados en la propuesta de resolución. Se acompaña documento 3 y link con el modelo de consentimiento informado actualizado. El modelo que aporta diferencia en un apartado “*mayores de 18 años*” y en el de “*menor de 18 años figura “y de sus representantes”* con espacio para rellenar los datos del alumno y del padre, madre o tutor. Señala la reclamada que “*dada la complejidad del tratamiento se va a solicitar que el consentimiento sea suscrito por el alumnado mayor de edad y, en el caso del alumnado menor de edad, por sus padres o representantes legales*”

Se ha añadido la posibilidad de que el consentimiento aquí otorgado podrá ser revocado en cualquier momento. Figura un link al “*RAT*” a través de gobiernocanarias.org.

Figura la identidad, dirección y contacto del responsable del tratamiento, información sobre el encargado de tratamiento y de que la transferencia de datos a GOOGLE está sujeta a clausula contractual tipo. Llevando a un link de GOOGLE que proporciona información sobre las CCT, incluyendo el acceso a un pdf de septiembre de 2022.

Se informa sobre la retirada del consentimiento y se indica que puede consultar información adicional y detallada en una dirección web del Gobierno de Canarias

3) Adjunta como documento 4 la elaboración y publicación del modelo de revocación del consentimiento que ha creado, así como el link.

4) Se ha creado en la web de la Consejería un apartado que contiene la “*segunda capa*” de información de la recogida y tratamiento de datos a los interesados, distinta al RAT. Aporta copia de documento 5 y link.

5) Se ha realizado un nuevo análisis de riesgos del tratamiento de “*solución de servicios digitales y telemáticos para la comunicación y la colaboración g suite*”.

Aporta documentos 6 “*metodología de análisis de riesgos*”. En él se indica que se ha confeccionado conforme a la guía de junio 2021 de la AEPD de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, excepto en la evaluación de impacto que acude a la guía de la Autoridad Catalana de protección de datos

Aporta copia de documento 7, “*informe de la aprobación del análisis de riesgos*” (11 páginas) en el que, además, ha participado el adjudicatario del contrato administrativo de servicios de adecuación al ENS. El análisis de riesgos se concreta en:

Archivo F 1, descripción del tratamiento y ciclo de vida de los datos personales,
Archivo F 2, evaluación del contexto,
Y archivo F 3, impacto y controles de seguridad.

Indicándose un link y una contraseña para acceder a cada uno de ellos, insertada da como resultado que “*está mal o ha caducado*” por lo que no se puede visionar el contenido.

Se ha realizado un nuevo informe de necesidad y evaluación de impacto del tratamiento en solución de servicios digitales y telemáticos para la comunicación y colaboración G Suite. Aporta documentos F 4 de EIPD con un link y contraseña, que no es posible abrir.

6) Aporta documento 8, *“informe de seguridad de la información”* del responsable de seguridad delegado, en el que indica que ha contratado servicios de consultoría y soporte para la adecuación al esquema Nacional de Seguridad y gestión de la seguridad de la Consejería, que se encuentra actualmente en fase de ejecución, donde se incluye expresamente el análisis de riesgos y evaluación de impacto de los entornos digitales o espacios virtuales de uso educativo que ofrece la Consejería a los centros públicos educativos y que implican el tratamiento de datos personales.

En el apartado *“3.2.1. Normativa, procedimientos y procesos de seguridad”*, se explicita que *“De acuerdo con el principio de proactividad establecido en el artículo 5.2 del RGPD, se deberán establecer los criterios, requisitos y medidas técnicas exigibles a las aplicaciones, plataformas o herramientas digitales de terceros de uso educativo para los centros educativos públicos de Canarias, que garanticen el cumplimiento de las medidas de seguridad y protección de datos personales.”* *“Como consecuencia de lo anterior, la empresa adjudicataria concretará una propuesta rigurosa en forma de protocolo o procedimiento de autorización a seguir por parte de la CEUCD, que se aplicará formalmente en un procedimiento de autorización de aquellas aplicaciones, plataformas o herramientas de terceros de uso educativo, que traten datos personales y que la CEUCD considere adecuadas para los procesos de enseñanza aprendizaje en los centros educativos públicos no universitarios de Canarias.”*

Se han valorado los activos e información de GSUITE educativo de la CEUCD, realizándose con la herramienta *PILAR* del Centro Criptológico Nacional los análisis de riesgos. De este análisis, se concluye que los activos asociados al G suite educativo de la CEUCD se encuentran dentro de un nivel de riesgo considerado aceptable para la CEUCD. Manifiesta que GS cumple con el ENS.

Aporta links a los archivos en los que se alojan los informes de *“valoración de servicios de información”*.

-En el documento 8, valorando la propuesta de resolución, se señala que se emitieron el 27/07/2021, antes de la presentación de la reclamación, unas recomendaciones en relación con el uso de aplicaciones y plataformas no corporativas por los centros educativos no universitarios dependientes del Departamento, reseñando extractos de su contenido.

7) Con fecha 16/09/2022, se publica la circular de la Dirección General de Ordenación, innovación y calidad de la CEUCD por la que se informa sobre el uso de aplicaciones de terceros no conveniadas a través del servicio G suite educativo y sobre el uso de sistemas de información y comunicación con la comunidad educativa en materia de protección de datos, donde se explicita lo siguiente:

“(…) los ajustes aplicados a la configuración del G Suite educativo de la Consejería de

Educación Universidades, Cultura y Deportes no permiten el acceso a aplicaciones de terceros no conveniadas, en las que el alumnado deba registrarse con su cuenta de usuario de G Suite educativo, con el fin de garantizar los derechos del alumnado en materia de protección de datos personales. (...)

“(...) En lo referido al uso de sistemas de información y comunicación con la comunidad educativa diferentes a los proporcionados por la CEUCD, se le remite a la Resolución de la Viceconsejería de Educación, Universidades y Deportes por la que se dictan instrucciones de organización y funcionamiento dirigidas a los centros docentes públicos no universitarios de la Comunidad Autónoma de Canarias para el curso 2022-2023, que recoge en su apartado 3.12. (...)”.

8) Se indica que se solicitó a GOOGLE información sobre su adaptación al ENS y este respondió que cumple el ENS proporcionando con una serie de links;

-El primero: *****URL.6**, explica lo que es el ENS y que GOOGLE CLOUD y GOOGLE WORKSPACE han acreditado su cumplimiento.

- <https://cloud.google.com/docs/security>, proporciona diversa información sobre seguridad entre otros puntos, como GOOGLE responde ante incidentes de datos en GOOGLE CLOUD, proteger cuentas en caso de credenciales vulneradas, uso de herramientas de GOOGLE CLOUD para ayudar a reducir el riesgo de robo de datos, o como se almacenan den la nube con GOOGLE KEY MANAGEMENT

-*****URL.7**, abre un archivo pdf (abril 20) que trata sobre seguridad y cumplimiento para GOOGLE WORKSPACE, refiriendo aspectos como el control del malware en los e mails y las herramientas de que dispone para contención y prevención.

*****URL.8**, que lleva a un archivo pdf de 37 páginas sobre Google workspace for Education, implementación de guía de protección de datos, de febrero 2023, indicando que GOOGLE actúa como encargado de tratamiento de los datos que le remite el cliente.

*****URL.9**, lleva a GOOGLE FOR EDUCATION, “Centro de privacidad y seguridad” con diversa información sobre protección de datos del centro educativo.

*****URL.10**

9) Se indica que el responsable de seguridad ha constatado que la aportación de evidencias por Google, muestran que al menos desde 16/10/2019, los sistemas de información para Google G Suite Services fueron auditados y encontrados conforme con las exigencias del esquema Nacional de Seguridad con categoría alta. El certificado se renovó el 18/11/2021. Aporta certificado, así como la fecha de la citada renovación. aporta copia de documento del centro Criptológico Nacional sobre seguridad y cumplimiento normativo de Google Classroom que es una aplicación que forma parte del paquete de herramientas de Google suite para la educación.

Aporta certificado de 18/10/2021 renovado con 18/10/2022 en lo que se indica que los sistemas de información que soportan los servicios de Google Workspace incluidos en el anexo y que se prestan desde los centros de Google localizados en Europa en diferentes países han sido auditados y encontrados conforme con las exigencias del Real decreto 3/2010 de 8/01 que regula el ENS.

Asimismo, menciona que cumple diversos estándares, como el ISO IEC 27017 de controles de seguridad de la información aplicables al uso de servicios en nube, el 27701 de procesador de información de identificación personal trabajo y las leyes de privacidad internacionales, y se enfoca en tres aspectos principales:

- Ampliar los requisitos de los estándares ISO/IEC 27001 e ISO/IEC 27002 para incluir la privacidad de datos.
- Proporcionar un marco de trabajo para la implementación, el mantenimiento y la mejora continua de un Sistema de Gestión de Información de Privacidad (PIMS).
- Incluir requisitos y lineamientos para las organizaciones que se desempeñan como controladores y procesadores de PII.

10) Acompaña informe en un link que se solicitó a GOOGLE, de un servicio auditor independiente, con información sobre Google Workspace (entre otros), si bien en ninguno de los dos links que señala aparece información al respecto. Manifiesta que Su utilidad es la de evaluar los riesgos que surgen de las interacciones con el sistema durante el período comprendido entre el 1/03/2022 y el 28/02/2023. En particular, proporciona información sobre los controles del sistema que Google ha diseñado, implementado y operado para brindar una seguridad razonable, y que sus *compromisos de servicio y los requisitos del sistema se cumplieron en función de los criterios de seguridad, disponibilidad y confidencialidad de los servicios de confianza establecidos en TSP Section 100 2017. Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (includes March 2020 updates). Se analizaron 129 controles y no se observaron desviaciones*

También se aportan links que remiten a salvaguardas para las transferencias, “*Safeguards for international data transfers with Google Workspace and Workspace for Education*” y “*GOOGLE CLOUD’s approach to European standard clauses,*” referido a septiembre 2022.

11) Aporta copia de informe del IES, como alegaciones a la propuesta en el que indica que se recibió el 27/11/2020 escrito del reclamante y se contestó el 3/12, pidiendo el 28/12 asesoramiento a la inspección informándole de las actuaciones a realizar que se han relatado anteriormente. Añaden que por la situación de emergencia de la COVID 19 en la época más compleja de la educación, su voluntad era la de garantizar la educación del alumnado, y sus acciones iban dirigidas en ese sentido, habiéndose corregido las irregularidades.

DÉCIMO PRIMERO: De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

1) El reclamante presenta reclamación ante la AEPD el 14/09/2021. Su hijo de 12 años se matriculó en el IES *****IES.1** en el curso 19/20 (primer año de estancia), y declara que tanto en ese curso como el siguiente, 20/21, se le dio de alta en el uso de la plataforma de educación *GOOGLE SUITE PARA LA EDUCACIÓN (GS)* sin su autorización. El reclamante indica que el 8/07/2020, entregó la matrícula de su hijo al IES *****IES.1** para el curso 20/21 (año en que aún no se había implantado la GSUITE de la Consejería) no dando el consentimiento para el uso de GSUITE que había implantado el IES sin autorización para ello de la CEUCD, responsable del tratamiento.

De acuerdo con la respuesta del IES al reclamado, entre otras, la de 28/12/2020, se deduce el alta en GSuite por el IES en el curso 20/21, con continuación de escrito del reclamante de 29/01/2021, *“eliminación de la cuenta de la plataforma” “al no contar con su consentimiento”* y certificado del IES de cancelación de la cuenta de correo electrónico que da soporte a GS, así como respuesta de 4/10/2021 del IES:

“El 16/01/2021, se procede a la eliminación de la cuenta por parte del coordinador TIC (por protocolo se queda 20 días en suspenso hasta su eliminación total).”, resultando la fecha de la baja pospuesta hasta el 7/07. *“Se informará al equipo educativo de **XXX-XX A**, que el alumno... no podrá utilizar más la herramienta GSUITE, establecida como entorno virtual de aprendizaje tipo reflejado en la PGA del centro”.*

2) La CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS-CEUCD, para los centros públicos docentes no universitarios de Canarias, contaba con el registro de actividad de tratamiento: *“Espacios virtuales de aprendizaje y colaboración”*, Orden departamental 185/2018 de 25/05/2018, que abarca alternativas de uso no obligatorio en combinación con la educación presencial, con el fin de dar respuesta a las necesidades educativas, tanto del profesorado como del alumnado. Se incluyeron como tales *“aulas virtuales”*, las aplicaciones *“EVAGD”*, *“CAMPUS”* y *“AULA DIGITAL CANARIA”*, todas ellas alojadas en servidores de la reclamada.

Como fines del tratamiento, se indican entre otros:

“Las enseñanzas a distancia dirigidas al alumnado, profesorado, familias y personal de administración y servicios.”

No se prevé la cesión de datos ni transferencias internacionales previstas.

3) La CEUCD firmó el 28/09/2020 un Convenio con GOOGLE IRELAND LIMITED dentro del Plan para la educación digital, *“para el uso de GOOGLE SUITE PARA LA EDUCACIÓN (GS) en los centros docentes públicos dependientes de la CCAA de Canarias”*, Boletín Oficial de Canarias 19/10/2020, complementando la oferta de plataformas educativas del *“entorno virtual de aprendizaje de gestión distribuida (EVAGD), y CAMPUS*, sin que suponga exclusividad del uso de este tipo de servicios digitales y telemáticos frente a otros similares. La CEUCD lo implementa para el curso

del año siguiente, 2021/2022, (9/09/2021 tercer año de estancia del alumno hijo del reclamante). Para ello, dispone de un modelo de “*consentimiento informado*” de uso y tratamiento denominado: “*solución de servicios digitales y telemáticos para la comunicación y la colaboración GSUITE*”, aprobado por resolución de la Dirección Gral. Ordenación, Innovación y Calidad el 11/09/2020, figurando en el link:

*****URL.11**

GS trata datos de alumnos y profesorado, nombre apellidos, correo, avatar del alumnado, CIAL (código interno de la CEUCD formado por 10 caracteres).

“Los servicios propios del GS hacen uso de diversos datos académicos y profesionales proporcionados por los usuarios: producciones del alumnado, calificaciones, grupos, materias...La finalidad del tratamiento de estos datos es el acceso al servicio del GS Educativo con fines estrictamente educativos, para apoyar las enseñanzas de los centros docentes públicos no universitarios de Canarias.”

En el apéndice 1 de la adenda de tratamiento de datos al acuerdo de Google suite, titulado objeto y detalle del tratamiento de datos se recoge como objeto la prestación por parte de Google de los servicios y del soporte técnico al cliente.

En su apartado 4 del Convenio se indica que resulta de aplicación la legislación europea de protección de datos cuando el tratamiento de datos se realiza en el contexto de las actividades de un establecimiento del cliente en el Espacio Económico Europeo o los datos personales del cliente se encuentran en el EEE. En el apartado 5 se indica que GOOGLE es un encargado de tratamiento de datos personales del cliente. En el apartado 5.2 “*alcance del tratamiento*” sobre instrucciones del cliente a GOOGLE.

En el apartado 7 titulado “*Seguridad de los datos*”, se indica que GOOGLE ha de adoptar medidas técnicas y organizativas para proteger los datos del cliente como se describe en el apéndice 3 “*Medidas de seguridad que incluyen el cifrado de datos, la ayuda para restablecer el acceso después de un incidente y que GOOGLE pondrá a disposición de los usuarios controles de seguridad adicionales para permitir que el cliente tome medidas para asegurar sus datos y proporcionar al cliente información sobre la seguridad del acceso y el uso de sus datos y que asistirá al cliente para garantizar el cumplimiento de sus obligaciones de conformidad con los artículos 32 a 34*”.

En su punto 7.5 se da la opción al cliente para recabar de Google informes para su revisión con el fin de demostrar el cumplimiento por parte de GOOGLE de sus obligaciones en virtud de la adenda del tratamiento. El punto 7.5.2 habilita que GOOGLE permita al cliente o un auditor externo por el designado, realice auditorias con el mismo objeto.

4) Manifiesta la reclamada que como base jurídica del tratamiento de datos personales realizados con la aplicación GSUITE suscrita a través del Convenio, implanta a partir del curso 21/22, se aplicaría el consentimiento previsto en el artículo 6.1.a) RGPD.

Además, manifestó que el tratamiento se fundamenta en el cumplimiento de obligaciones legales y en el ejercicio de poderes públicos conferidos al responsable del tratamiento, mencionando diversos artículos de diversas leyes referidas a la competencia digital.

5) De acuerdo con la información aportada por el reclamante, el IES ofrecía en la web para el curso 21/22 (año de implantación de GS-Convenio GOOGLE CEUCD) un *"manual de acogida"*, con información sobre el contenido de la plataforma GS para la educación, en el sentido de que el centro educativo solo y únicamente debe dar de alta el servicio al alumnado, si está en posesión del documento de consentimiento informado de las familias *que han firmado aceptando las condiciones de participación figurando un link al citado documento de "consentimiento informado"*. GS según la reclamada es una herramienta con fines educativos para apoyar las enseñanzas de los centros docentes públicos no universitarios. En el mismo link hay un apartado de *"Preguntas frecuentes"*, del que se acredita que los centros han usado previamente GS, dado que se informa:

"Si ya tenemos funcionando una cuenta de Google, con dominio de centro, ¿puedo seguir utilizándola?", y otra sobre la exportación de la estructura actual de GS del centro a la nueva GS de la Consejería, o al consentimiento que se debió haber otorgado en su día al centro para el uso de dicho servicio.

También se informa que en virtud del Convenio GOOGLE/CEUCD, existe un registro de actividades de tratamiento (RAT) denominado *"solución tecnológica para la comunicación y la colaboración g suite"*, RAT que antes con los centros no existía según las preguntas frecuentes. La finalidad del tratamiento de estos datos es el acceso al servicio del G Suite Educativo con fines estrictamente educativos, para apoyar las enseñanzas de los centros docentes públicos no universitarios de Canarias.

6) También le consta a la CEUCD y aporta en previas (documento 1) el: *"No consentimiento de los padres o tutores" a través del "formulario de consentimiento informado" a los servicios G SUITE for EDUCATION*, del reclamante, fechado en 9/09/2021, curso 21/22 sobre la actividad de tratamiento: *"solución de servicios digitales y telemáticos para la comunicación y la colaboración G SUITE"*. Se acredita que en el citado curso no se trataron los datos del hijo del reclamante, si bien el reclamante puso de manifiesto deficiencias en la información de recogida de datos del consentimiento informado.

7) El modelo de *consentimiento informado* del curso en que se implanta GS por la Consejería, año 21/22, figura aportada el 18/02/2022 como documento 2 por la reclamada en actuaciones previas, al que se puede acceder en la dirección:

***URL.1

Además de informar, se autoriza el uso y tratamiento de los datos personales incluidos en la actividad de tratamiento *"solución tecnológica para la comunicación y la colaboración g suite"*, con dos casillas, una: *"consiente"*, otra: *"no consiente"*.

El modelo del documento no contenía:

- los datos de contacto del responsable, ni los datos de contacto del DPD.
- en ejercicio de derechos, no se menciona *"la existencia del derecho a retirar el consentimiento en cualquier momento"*
- destinatarios o categoría de destinatarios de los datos personales en su caso.

- *“en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.”*

- *“si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;”*

Si bien ofrecía consultar información adicional remitiendo a un link, este lleva al “Registro de actividad de tratamiento” integro, que se aprobó el 11/09/2020, que contiene (doc 6 de actuaciones previas) entre otros:

-datos del contacto responsable y del nombramiento de DPD, aunque faltan sus datos de contacto.

-No se prevé cesión de datos.

-En transferencias internacionales, solo figura que se autoriza a GOOGLE IRELAND mediante Convenio con la CEUCD.

En alegaciones al acuerdo, en el RAT actualizado -documento 6 A, pdf 2-que aporta la reclamada, siguen faltando las informaciones sobre especificidades de las transferencias internacionales, y agrega en la base jurídica, además del consentimiento, (que ha indicado que si no se otorga, no han de tratarse los datos del menor, al ser una herramienta complementaria a las clases presenciales, no la única y de uso voluntario), los artículos 6.1.c) *“el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”* y el 6.1.e), *el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;* del RGPD el 2.1.i) de la LO 2/2006 de 3/05 de Educación y el 24 de la Ley 6/2014 de 25/07 Canaria de educación no universitaria.

También falta la información de *“si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;”*

En alegaciones a propuesta de resolución se ha completado en el modelo de consentimiento informado la referencia a las transferencias internacionales y la opción de retirar el consentimiento, así como las consecuencias de no otorgar el consentimiento.

8) El alta de la gestión de cuentas del alumnado en el GS se puede llevar a cabo por el equipo directivo desde la consola de servicios del CAUCE (centro de atención de usuarios de la Consejería de Educación), *“siempre y cuando tenga firmado el documento de consentimiento informado de las familias”*, en la sección *“gestión de cuentas del alumnado”*, apareciendo el listado de todo el alumnado, debiendo seleccionarle para solicitarle su cuenta del GSUITE y enviar su solicitud. Para desactivar la cuenta, realizará la misma operación.

9) La reclamada no aportó copia del contrato suscrito por IES *****IES.1** con GOOGLE para el uso de GOOGLE SUITE que ha estado utilizando los cursos 19/20 y 20/21, indicando que tuvo que buscar un sistema para garantizar que se pudieran dar clases durante la declaración de la pandemia de la COVID 19. El reclamante añadió que tuvo dificultades para obtener copia del contenido de las materias de ese último año.

No consta que el IES al implantar GS realizara análisis de riesgos del tratamiento sobre el uso de datos personales con GS.

La Orden de 23/05/2019, por la que se aprueba la política de dominios en internet de la Administración Pública de la Comunidad Autónoma de Canarias, estableció que los centros educativos no pueden disponer de dominios propios distintos de los corporativos autorizados.

Para el uso de GS, se ha de disponer de un dominio propio. La CEUCD utilizó para el GS del Convenio, año de inicio, curso 21/22, un dominio propio para todo el ámbito de la misma: *****DOMINIO.1**. El año anterior, curso 20/21, el IES al utilizar GS *lo hizo con la cuenta del dominio ieslalaboraldelalaguna.es*, según consta en respuesta del IES de 4/10/2021 al reclamante, o comunicaciones sobre eliminación de las cuentas del dominio *ieslalaboraldelalaguna.es al alumnado al finalizar el curso escolar 20/21 y como transferir los contenidos de la GS antigua a la nueva*. *“El 7/07/2021, se realiza la eliminación definitiva de la cuenta del alumno B.B.B.”, “a mediados de septiembre se procederá a la eliminación de las cuentas actuales de Gsuite, para asignar las nuevas del curso 2021/22.” (según correo del IES de 18/06/2021)*

10) La reclamada aportó en previas una EIPD sobre la *“solución tecnológica para la comunicación y la colaboración GS”*, de 4/05/2021, después de publicado el Convenio (19/10/2020) cuando aún no había sido puesto en funcionamiento la herramienta GS, que se lleva a cabo en el curso 21/22, sirviéndose de la herramienta de la web de la AEPD: *“GESTIONA EIPD”* orientada para PYMES” según la web de la AEPD. En el documento realiza un análisis de riesgos sobre GS finalizando con riesgo aceptable. En el documento no se produce una específica identificación de riesgos, partiendo de 32 apartados usados para *“evaluación del nivel de riesgo”*. La valoración de los riesgos tiene en cuenta “medidas” no contemplan la relación jurídica de encargo de tratamiento específica con GOOGLE y las herramientas diversas que se utilizan para el tratamiento (Gmail, DRIVE, Classroom, doc)

11) En alegaciones a la propuesta la reclamada ha modificado el análisis de riesgos del uso de GS con una nueva metodología, si bien la parte del resultado del análisis no se ha podido comprobar por no poderse abrir los archivos que remitieron. En el mismo sentido con la EIPD modificada. Además, indica que en la actualidad se está en la última fase de ejecución de un contrato de servicios de adecuación al esquema del ENS en el que se incluye el análisis de riesgos y evaluación de impacto de los entornos digitales o espacios virtuales de uso educativo que ofrece la Consejería a los centros públicos educativos y que implican el tratamiento de datos personales.

12) La reclamada comenzó a dictar instrucciones y circulares sobre el uso de plataformas educativas y aplicaciones no corporativas por los centros educativos el 27/07/2021

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 5/12 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 registrarán 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

El RGPD indica:

artículo 1:

"1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales."

artículo 3:

"1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

artículo 4:

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona 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;

2) «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;

[...]

7) «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;»

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

GOOGLE SUITE EDUCATION, en la actualidad GOOGLE WORKSPACE, es un paquete de servicios de la suite de *Google* basados en la nube, que permiten la edición colaborativa de documentos y la comunicación al instante desde cualquier dispositivo y lugar y que cobró protagonismo a raíz del inicio de la pandemia como herramientas de comunicación en los centros educativos por la ausencia o insuficiencia de los medios con que contaban los responsables del tratamiento.

Los servicios digitales de *GOOGLE SUITE* para la educación están vinculados a cuentas de correo electrónico asociadas a dominios de instituciones educativas. Normalmente, la Consejería de Educación como responsable del tratamiento es la que crea un dominio para la gestión de estas cuentas para los centros educativos. En el caso de CCAA de Canarias se creó el dominio canariaseducación.es para la gestión de esas cuentas para los centros educativos de titularidad pública, impidiendo la proliferación de que cada centro, instituto, colegio o escuela que dispusiera de un dominio tipo @nombredelcentro.org y gestionara por separado su cuenta. Una vez creado el dominio canariaseducación.es se crearían cuentas de correo ligadas a ese dominio para el profesorado y el alumnado. Cada usuario cuenta con una dirección de correo electrónico asociado a los servicios digitales.

Al iniciar sesión en cualquiera de las aplicaciones *Google*, se accede mediante la cuenta de correo electrónico asignada y su contraseña, se accede a todo el contenido de servicios que ofrece *Google Suite*.

Los servicios y configuraciones se realizan desde la “consola de administración”, “herramienta y consola online que *Google* pone a disposición del cliente para administrar los servicios.”

Esto incluiría opciones de seguridad en la configuración de las cuentas, de los buzones y de los mensajes.

La aplicación tiene varias ediciones, siendo la básica “*FOR EDUCATION FUNDAMENTALS*”, gratuita para las instituciones que cumplan los requisitos. En esta versión no se incluyen servicios adicionales tal como se recoge en el Convenio, sin embargo,

en la información del consentimiento para el tratamiento se introduce información sobre tales servicios, pudiéndose dar información que no se corresponde con la realidad.

La cuenta del cliente es alojada por GOOGLE.

La disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3/05, de Educación, establece de modo general, uno de los principios básicos en relación con el tratamiento y comunicación de datos de carácter personal dentro de su ámbito de aplicación, al disponer:

“3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.”

El Comité Europeo de Protección de Datos ha recogido en las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 versión 1.1 adoptadas el 4/05/2020, que, *“para obtener el consentimiento informado válido, al menos, se deberá facilitar a los interesados la información siguiente: «i. la identidad del responsable del tratamiento, ii. el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento, iii. qué (tipo de) datos van a recogerse y utilizarse, iv. la existencia del derecho a retirar el consentimiento, v. información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente, y vi. información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas, tal y como se describen en el artículo 46”*. Añade el Comité que *“un responsable del tratamiento que se base en el consentimiento del interesado deberá también abordar las obligaciones de información separada establecidas en los artículos 13 y 14, con el fin de cumplir con lo estipulado en el RGPD. En la práctica, el cumplimiento de las obligaciones relativas a la información y el cumplimiento con el requisito del consentimiento informado pueden conducir en muchos casos a un planteamiento integrado (..)”*

En este caso, en cuanto al cumplimiento del derecho de información a los afectados en la recogida de datos, en relación con el convenio con Google, publicado en el Diario Oficial el 20/10/ 2020, e implantado en el curso 21/22, se aprecia que de la documentación aportada por CEUCD no se acredita que haya facilitado a los interesados toda la información prevista en el artículo 13, ni integrada en la cláusula utilizada para la obtención del consentimiento ni en otro lugar. La cláusula de consentimiento informado utilizada por CEUCD carece de algunos elementos informativos que deben facilitarse al interesado en el momento de la recogida de sus datos que se indican el artículo 13 del RGPD que señala

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
- b) los datos de contacto del delegado de protección de datos, en su caso;*

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4.Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información”

Así, el “formulario de consentimiento informado” carecía, antes del acuerdo de inicio de:

-datos de contacto del responsable.

-datos de contacto del DPD.

-el derecho a presentar una reclamación ante la autoridad de control,

-información sobre la transferencia internacional de datos, *“en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.”*

-destinatarios o categorías de destinatarios de los datos personales, en su caso.

- *“cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;”*

- *“el derecho a presentar una reclamación ante una autoridad de control”*

- *“si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos”*

Acudiendo al link que figuraba como información adicional, se accede al registro de actividad de tratamiento integro, esto es, la resolución de la D. Gral. que registra la actividad de tratamiento *“solución tecnológica...”* documento 6 de actuaciones previas. Al respecto se debe indicar que la cláusula está implementada para menores de edad que pueden otorgar el consentimiento y para los que la lectura de todo el contenido del RAT no resulta adecuada por su nivel de comprensión ni parece clara y sencilla. En cuanto al contenido de la información referida al artículo 13, el RAT ofrecía información de:

-datos de contacto del responsable del tratamiento.

-datos de contacto del DPD: aunque identifica los designados como tales, no establece el contacto, ni el medio, ni una dirección, no considerándose que contiene tal dato de contacto.

-Establece que no se prevé cesión de datos.

-Establece solo, que se autoriza a GOOGLE mediante convenio con la CEUCD la transferencia de datos, sin añadir los detalles que se contiene en el precepto.

Tras recibirse el acuerdo de inicio, la reclamada ha introducido en el *“formulario de consentimiento informado”*, las siguientes modificaciones:

- “Derecho a reclamar ante la autoridad de control: La AEPD es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos, y un link para la Presentación de reclamaciones ante la sede electrónica de la AEPD.

-Datos de contacto de los DPD.

-Sigue sin completar los aspectos de la retirada del consentimiento ni la totalidad de información referida a las transferencias internacionales.

-Sigue identificando a responsable del tratamiento, pero ignora los datos de contacto.

-Sigue sin indicar si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;

-Otro link remite a información adicional, que contiene la resolución de la Dirección Gral. de Ordenación, Innovación y Calidad de 11/09/2020, por la que se actualiza el registro de las actividades de tratamiento de datos personales a 26/09/2022, “*SOLUCIÓN TECNOLÓGICA PARA LA COMUNICACIÓN Y LA COLABORACIÓN G SUITE*” (documento 6 A del pdf 2) en la que en el seno de la información del RAT, se dan los datos de contacto del responsable.

En las alegaciones a la propuesta, la reclamada ha completado la información de la recogida introduciendo la retirada del consentimiento, sobre las transferencias y las consecuencias, junto a la identificación de contactos y DPD, cambiando el link de la segunda capa, quedando subsanada la infracción, si bien en el momento de iniciar el procedimiento quedó acreditada la comisión de la infracción imputada.

III

En cuanto al ámbito de implantación de GOOGLE SUITE PARA LA EDUCACIÓN, a través del Convenio suscrito, se aprecia que el análisis de riesgos se efectúa a través de la aplicación “*GESTIONA EIPD*” el 4/05/2021.

No obstante, se constata que el análisis de riesgos no toma en consideración a título de ejemplo:

-En “*descripción del tratamiento*”, no se alude intrínsecamente a la solución tecnológica, en la que cada herramienta puede implicar un riesgo diferenciado, como el uso y tratamiento en la nube, el de g mail, herramientas de compartir como *DRIVE*, etc., o a la opción de retirar el consentimiento y la exportación de datos, por poner solo algunos ejemplos.

-Los riesgos que se analizan no son específicos del tratamiento, sino los genéricos que forman parte de un listado de la aplicación “*GESTIONA EIPD*” que la AEPD ofrece como herramienta básica gratuita en su web. Se recogen directamente el listado de riesgos de dicha herramienta sin identificar antes los riesgos propios de la aplicación.

-El análisis de riesgo no se ha realizado por la Consejería teniendo en cuenta los riesgos puestos de manifiesto por su encargado. No contempla los riesgos inherentes de la aplicación para los derechos y libertades de las personas ni cómo los gestiona Google, lo que impide que puedan tomarse medidas adecuadas a tales riesgos, como los riesgos para los menores.

Así, de acuerdo con el considerando 83 del RGPD “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”, lo que no consta que se haya realizado en este caso.

Sobre la herramienta GESTIONA EIPD, la guía de la AEPD de “gestión del riesgo y evaluación de impacto en tratamiento de datos personales de junio de 2021” indica: “... la AEPD ha publicado la herramienta GESTIONA EIPD, que guía a los usuarios a través de los elementos básicos que deben ser tenidos en cuenta en los análisis de riesgos de los tratamientos y en las evaluaciones de impacto. Esta herramienta proporciona las bases mínimas para iniciar las actividades de gestión de riesgos en el ámbito del RGPD, incluyendo requisitos de cumplimiento normativo con el fin de permitir a pequeñas y medianas empresas, que no dispongan de un marco para la gestión del riesgo en su organización, iniciarse en las labores de identificación, evaluación, gestión de los riesgos de los tratamientos de datos personales y ejecución de EIPD.”

En la web de la AEPD, sobre GESTIONA, se añade:

“Gestiona, en su estado de evolución, es el punto de partida para comenzar la gestión del riesgo”.

“Sobre la base de los documentos obtenidos los responsables y encargados de los tratamientos de datos personales deberán llevar a cabo cuantas adaptaciones fueran necesarias de forma particularizada para cada tratamiento de datos personales; teniendo en cuenta los riesgos que para los derechos y libertades de las personas físicas pudieran derivar de dichos tratamientos en función de su naturaleza a su alcance su contexto y sus finalidades considerando 76 y artículo 35.1 del RGPD.

Gestiona EIPD es una herramienta de ayuda y soporte a la decisión y cuya utilización genera la documentación básica y en ningún caso exhaustiva sobre la cual hay que realizar un análisis y gestión del riesgo por parte de las personas responsables y encargadas para cumplir con lo previsto en el RGPD y la LOPDGDD.

Esta documentación básica será un punto de partida que deberá ser completada y analizada por el personal responsable del tratamiento y, en su caso, la persona encargada, siguiendo las indicaciones establecidas en la guía de gestión de riesgo y evaluación de impacto en tratamiento de datos personales, con el fin de demostrar en todo momento que los tratamientos se llevan a cabo de conformidad con los requisitos.

Gestiona EIPD está orientada a PYMES”.

En relación con lo anterior, dada la especificidad del ámbito educativo y el tratamiento de menores de edad, y el tipo de aplicación con todas las herramientas de que dispone GESTIONA no tiene en cuenta estas circunstancias en el básico análisis de nivel de riesgos realizado por la reclamada.

-Se aprecia que las amenazas-riesgos, (31) podrían ser unos mínimos, no son específicos y concretos, pudiendo ser comunes a multitud de tratamientos y una serie de ellos relacionados con los principios del artículo 5 del RGPD más relacionados con el cumplimiento normativo. El considerando 84 del RGPD señala que la evaluación ha de ser en particular sobre el origen, la naturaleza, la particularidad y a gravedad de dicho riesgo

-Si bien se indica que los datos personales que la CEUCD facilita a Google son mínimos y por tanto constituyen “*un riesgo bajo*”, no se refieren los eventuales datos que derivarían del uso de la aplicación, como imágenes, formularios, sonidos, adjuntos de emails, calificaciones que efectúan los profesores, producciones que realizan los alumnos, a título de ejemplo, ni los tratamientos que realiza GOOGLE para prestar el servicio y sus riesgos.

-La reclamada ha aportado certificado con el sello de ENAC de conformidad de GOOGLE SUITE con el ENS, e informe del Centro Criptológico Nacional sobre la aplicación GOGLE CLASSROOM, que forma parte de GSUITE, en el que se indica que tiene la conformidad para el ENS de nivel alto.

El artículo 156.2 de la LRJSP, indica sobre el mismo:

“2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.”

Por otro lado, se ha de tener en cuenta que el Real Decreto 3/2010, de 8/01, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, dispone en su artículo 1.2 que “*El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias*”.

Sin embargo, el RGPD demanda la identificación, evaluación y mitigación del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos. Estas deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento. Además, dichas medidas se revisarán y actualizarán cuando sea necesario. En definitiva, el RGPD exige un proceso de gestión del riesgo para los derechos y libertades de los interesados que va más allá de lo que contempla el ENS.

Además, los riesgos se producen a través de la aplicación que utilizan los alumnos cuando acceden y operan en la misma, no sobre los activos de la propia entidad. El ENS contiene principios básicos y requisitos mínimos para una protección adecuada de la información para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

No se tiene en cuenta las medidas de seguridad que adopta el encargado de tratamiento, aunque algunas de ellas constan en el Convenio, y las que la reclamada puede exigir de modo adicional como responsable del tratamiento y el control que sobre las mismas puede revisar o proponer.

-Somera e insuficiente referencia al riesgo de tratamiento de las transferencias internacionales, y a las medidas.

-Las conclusiones a que llega del análisis del riesgo en cuanto a probabilidad, impacto, riesgo residual aparecen sin explicación, y no guardan lógica, ejemplo riesgo de fuga de información: riesgo medio, y violaciones de confidencialidad de datos por parte de empleados o personal externo: bajo, manipulación o modificación no autorizada de la información que se centra solo en la gestión del registro de usuarios: bajo.

-Descripción incompleta o parcial de las “amenazas riesgos”. Simplificación del apartado “medidas” que lleva a considerar el resultado en probabilidad/impacto riesgo residual.

-Especificaciones sobre los usos y posición jurídica de las partes en los servicios adicionales (you tube, maps, photos) si se implementan, aunque en el Convenio se significa que están fuera de la versión gratuita, la usada por la reclamada.

-Se efectúan accesos a la plataforma GS a través de la creación de una cuenta de correo electrónico Gmail para los alumnos, sin determinar los riesgos para los derechos y libertades y el impacto que puede tener en los mismos.

-Los riesgos y garantías del funcionamiento en la nube de los datos almacenados.

-Configuraciones por defecto que no pueden ser variadas o si, dependiendo de la edad.

-Tratamientos y riesgos según edades de videos o grabación de clases por video.

-Escasa explicación del riesgo en las transferencias internacionales de datos.

-Falta de colaboración de GOOGLE como encargado del tratamiento en la valoración de los riesgos.

Los considerandos 74 y 78 del RGPD señalan:

“(74) 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 cuanto a los riesgos que manifiesta la reclamada se evaluaron en 2018 y 2019, aparte de que se centran en el ENS, y sobre las actividades virtuales, no contenían las del uso de GS en el IES (año 2019 y 2020), ni se evalúan los riesgos para los derechos y libertades de las personas.

El análisis de riesgo sobre la aplicación GSUITE se estima incompleto en la unidad de estructura que conlleva la imputación de dichas infracciones, subsumiéndose en el que contiene las carencias expresadas.

Por ello, se considera que la reclamada infringió el RGPD en el artículo 32 del RGPD, que indica:

“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.”.

IV

En cuanto al tratamiento de los datos del hijo del reclamante en los años 2019/2020, y siguiente, 2020/2021 por el IES, y anteriores a la implantación del Convenio, el RGPD considera responsable del tratamiento, de acuerdo con el artículo 4.7 del RGPD:

“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;”

Es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

En este supuesto, fue el IES el que decidió la contratación de GS, ejerciendo una influencia determinante en el tratamiento, sin que existiera registro de actividad de tratamiento, como lo certifica la aprobación por la Consejería del RAT *“solución tecnológica para la comunicación y la colaboración G SUITE”*.

Se debe aclarar que la infracción de la falta de legitimación imputando el artículo 6.1 del RGPD no lo es por el Convenio GOOGLE-CEUCD, sino por el uso en dos años consecutivos por parte de un IES, que carece de la condición de responsable del tratamiento y en consecuencia de competencias como responsable del tratamiento, de la herramienta antes de la aprobación del Convenio y de la implementación de la herramienta.

El RGPD señala en su artículo 5.2:” *El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 (principios del tratamiento entre los que se encuentra el modo en que han de ser tratados los datos, “de manera lícita, leal y transparente”) capaz de demostrarlo («responsabilidad proactiva»)*. Ello implica que el citado responsable es el que asume su propia responsabilidad dirigiendo y coordinando la materia, incluyendo la del personal que le presta servicios.

No consta que la aplicación de la plataforma en el IES fuera complementaria como si se señala en el acuerdo suscrito por la Consejería. En la implantación por el IES, según se desprende, el reclamante, no proporcionó el consentimiento, si bien se le dio de alta en la plataforma, y fue el consentimiento el que se utilizó como base legitimadora.

Con la creación de la cuenta por el IES de GS para educación, usando un dominio propio, se asignó a cada alumno un usuario y contraseña que les permite, entrar en la solución GS, iniciando sesión en cualquiera de las aplicaciones *Google*. Su uso puede efectuarse desde distintos dispositivos al funcionar en la nube, se precisa acceso a internet.

Los servicios y configuraciones se realizan desde la “*consola de administración*”, “*herramienta y consola online que Google pone a disposición del cliente para administrar los servicios.*”

La aplicación tiene varias ediciones, siendo la básica “*FOR EDUCATION FUNDAMENTALS*”, gratuita para las instituciones que cumplan los requisitos. La cuenta del cliente es alojada por GOOGLE.

Se considera que La Consejería resulta responsable del tratamiento de los datos del hijo del reclamante sin base jurídica, infringiendo el artículo 6.1 del RGPD, que señala:

“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.”

El artículo 7 del RGPD indica: “*Condiciones para el consentimiento*”:

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.”

Todo ello, atendiendo a lo que establece el artículo 7 de la LOPDGDD, sobre el consentimiento de los menores de edad (18 años) que señala:

“1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

1. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.”

La reclamada no realiza alegación alguna sobre este aspecto, reconociendo en alegaciones a la propuesta que implantó un sistema para seguir dando clase, por la irrupción de la pandemia, indicando que dio las órdenes al IESA para que usara las aplicaciones que hubieran sido aprobadas por ella.

Para el uso de GOOGLE SUITE cabe diferenciar entre los menores de 14 años y los mayores de esta edad que han de prestar por sí mismos el consentimiento. En este caso el reclamante no había prestado el consentimiento para el tratamiento de los datos de sus hijos menores de 14 años.

Por otro lado, no consta que, para dicha implementación, se efectuaran análisis de riesgos, tal como prevé el artículo 32 del RGPD y que incide en las medidas de seguridad, estimándose que ha infringido dicho artículo, por cuanto las medidas técnicas y organizativas apropiadas lo son en función de los riesgos para los derechos y libertades de las personas físicas con el fin de garantizar un nivel de seguridad adecuado al

riesgo. En este caso, no constan tales medidas que debieron ser implantadas, asimismo, por el responsable del tratamiento, en este caso la reclamada como entidad competente.

V

Las infracciones se incluyen en el artículo 83.4.a) y 83.5.a) del RGPD, que indica:

“4. 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;”

“5. 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;”

b) los derechos de los interesados a tenor de los artículos 12 a 22;”

El artículo 58.2 del RGPD indica:” Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

“d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado”.

El artículo 83.7 del RGPD añade:

“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.”

El ordenamiento jurídico español ha optado por no sancionar con multa a las entidades públicas, tal como se indica en el artículo 77.1. c) y 2. 4. 5. y 6. de la LOPDDGG: “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.

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.”

VI

A efectos de prescripción, la LOPDGDD indica:

Artículo 72. Infracciones consideradas muy graves:

“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:

“b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.”

El artículo 73 de la LOPDGDD indica:” *Infracciones consideradas graves”:*

“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.”

El artículo 74 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:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.”

VII

El artículo 58.2 d) del RGPD, señala que cada autoridad de control podrá “ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...”. La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En este caso, no se acredita que la reclamada haya realizado un análisis de riesgos en los términos expuestos en el fundamento III de la presente resolución.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS**, con NIF S3511001D, por las infracciones del RGPD en sus artículos:

- 13 del RGPD, de conformidad con el artículo 83.5.b), del RGPD, y a efectos de prescripción como leve en el artículo 74.a) de la LOPDGDD.
- 32 del RGPD, de conformidad con el artículo 83.4 a) del RGPD, y a efectos de prescripción como grave en el artículo 73. f) de la LOPDGDD,

- 6.1 del RGPD, de conformidad con el artículo 83.5 a) del RGPD, y a efectos de prescripción como muy grave en el artículo 72.1.b) de la LOPDGDD. multa de [Introduzca el texto correspondiente a

SEGUNDO: NOTIFICAR la presente resolución a **CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS.**

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

CUARTO: ORDENAR a **CONSEJERÍA DE EDUCACIÓN, UNIVERSIDADES, CULTURA Y DEPORTES DEL GOBIERNO DE CANARIAS**, con NIF S3511001D, que en virtud del artículo 58.2.d) del RGPD, en el plazo de un mes desde su recepción, acredite haber procedido al cumplimiento de las medidas para completar la información en el análisis de riesgos sobre G SUITE educativo que constituye el elemento esencial de la infracción del artículo 32 del RGPD

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 LPACAP. 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.

938-010623

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