CONSEJERÍA DE EDUCACIÓN Y UNIVERSIDADES

IES INGENIO

Protocolo de Protección de Datos

CURSO 2018/2019

Contenido

Información básica sobre Protección de Datos		
RESPONSABLE	IES INGENIO: 35010506 Avenida de los Artesanos, 55 Ingenio 35250 Islas Canarias. España; Teléfono: +34 928784600	secretariaiesingenio@gmail.com
FINALIDAD	La LOMCE legitima a los centros a recabar datos de carácter personal para la función docente y orientadora de los alumnos en referencia a: • n El origen y ambiente familiar y social. • n Las características o condiciones personales. • n El desarrollo y resultados de su escolarización. • nLas circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos	a) Gestionar las solicitudes de admisión y matriculación en el IES INGENIO b) Control y gestión administrativa, gestión de cobros y pagos a alumnos. c) Acciones que sean necesarias para la atención, evaluación y seguimiento académico de los alumnos. d) Plataformas Educativas e)Realizar entrevistas, evaluaciones psicopedagógicas que permitan orientar sobre la oferta educativa más adecuada a las necesidades del alumno y la emisión de dictámenes de escolarización. f) Envío de comunicaciones personalizadas por su condición de alumnado para informarle sobre servicios, productos o novedades relacionadas con nuestra actividad. g) Realización de encuestas de satisfacción y tramitación de hojas de reclamaciones y sugerencias. h) Informes de salud: ***En la matriculación del alumno***: discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias o alergias. ***Durante el curso escolar:*** el tratamiento médico que reciba un alumno a través del servicio médico o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.
LEGITIMACIÓN	La base del tratamiento de sus datos personales es el consentimiento necesario que se presta para la ejecución de la matrícula así como par a el cumplimiento de una obligación legal. Los datos que le solicitamos son adecuados, pertinentes y estrictamente necesarios y en ningún caso está obligado a facilitárnoslos, pero su no comunicación tendrá como consecuencia que su matrícula no pueda realizarse.	• La Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa (LOMCE). • Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, aplicable a partir del 25 de mayo de 2018).
DESTINATARIOS	Todos los usuarios del sistema educativo que realicen matrícula en el IES INGENIO.	Le informamos que los datos facilitados permanecerán en el aplicativo creado por la Consejería de Educación del Gobierno de Canarias (Pincel EKADE) con el fin de extender los certificados correspondientes y conservar los datos relativos a su escolarización en nuestra Comunidad Autónoma. No se transmitirán ni cederán datos a países no comunitarios (en el caso de realización de

		programas educativos europeos) ni a aquellos países catalogados por la UE como *no fiables.* No se cederán datos a terceros excepto en el cumplimiento de las obligaciones legales establecidas en el seno de la cooperación entre administraciones.
DERECHOS	· **Acceso**: para consultar sus datos personales que usted nos ha facilitado. · **Rectificación**: podrá modificar sus datos personales cuando sean inexactos o para su actualización. · **Supresión**: podrá solicitar la eliminación de sus datos personales, siempre que no afecte a la escolarización del alumno/a matriculado en el centro.	Se puede ejercer tales derechos en cualquier momento previa solicitud al correo proporcionado por el centro educativo.
PROCEDENCIA	Los datos personales, sanitarios, de condición y escolarización serán proporcionados directamente por las familias y/o por las otras administraciones educativas.	Se incorporarán al fichero personal de cada alumno/a

A. INFORMACIÓN GENERAL

A.1 ¿Qué es un dato de carácter personal?

Cualquier información alfanumérica, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Aunque no esté asociada a una identidad, es un dato de carácter personal si a través de dicha información se puede identificar o individualizar dentro de un colectivo a una persona sin esfuerzos desproporcionados.

A.2 Datos especialmente protegidos

Algunos de los datos personales son especialmente sensibles por revelar circunstancias o información de las personas sobre su esfera más íntima y personal. Requieren que se les preste una especial atención y se adopten las medidas técnicas y organizativas necesarias para evitar que su tratamiento origine lesiones en los derechos y libertades de los titulares de los datos.

Forman parte de esta categoría de datos personales aquellos que:

- revelen ideología, afiliación sindical, religión y creencias,
- hagan referencia al origen racial, a la salud y a la vida sexual,
- se refieran a la comisión de infracciones penales o administrativas.

En el ámbito educativo es frecuente, sobre todo, el tratamiento de datos relativos a la salud física o mental de los alumnos, incluida la prestación de servicios de atención sanitaria que revelan información sobre su estado de salud.

A.3 Tratamiento de datos en el IES INGENIO

La recogida de los datos de los alumnos y de sus padres al inicio del curso escolar es un tratamiento de datos de carácter personal.

Igualmente lo es el mantenimiento y la actualización del expediente del alumno y su transmisión a un nuevo centro en caso de traslado, así como la captación y grabación de imágenes a través de sistemas de videovigilancia.

A.4 Responsable del tratamieto de datos en el IES INGENIO

El responsable del tratamiento es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal.

Cuando se trate de centros educativos públicos, el responsable del tratamiento será normalmente la Administración pública correspondiente: la Consejería de la Comunidad Autónoma competente en materia educativa.

Se ha creado en cada centro la figura del responsable de la protección de datos, centrada en la persona que ostenta la secretaría del centro.

Es necesario que el tratamiento de datos que implica la prestación del servicio se rija por un contrato que deberá incluir las garantías adecuadas:

- La obligación del encargado del tratamiento de tratar los datos únicamente conforme a las instrucciones del centro o Administración educativa que ostente en cada caso la condición de responsable del tratamiento.
- Que los datos no se utilizarán para finalidades distintas de las previstas en el contrato, ni se comunicarán a otras personas, ni siquiera para su conservación.
- Las medidas de seguridad a implantar por el encargado del tratamiento.
- La devolución de los datos al centro o a la Administración educativa que sea responsable o al encargado del tratamiento que ésta designe o, en su defecto, su destrucción una vez finalizado el contrato.

No se consideran encargados del tratamiento a las personas físicas que tengan acceso a los datos personales en su condición de empleados del centro o de la Administración educativa que son los responsables del tratamiento.

B. TIPO DE DATOS

Las leyes educativas legitima a los centros a recabar datos de carácter personal para la función docente y orientadora de los alumnos en referencia a:

- El origen y ambiente familiar y social.
- Las características o condiciones personales.
- El desarrollo y resultados de su escolarización.
- Las circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos.

Por tanto, la LOE legitima a los centros educativos para recabar y tratar los datos de los alumnos y de sus padres o tutores, incluyendo también las categorías especiales de datos, como los de salud o de religión, cuando fuesen necesarios para el desempeño de la función docente y orientadora.

Pero también hay que tener en cuenta una serie de cautelas:

- Los datos personales no podrán usarse para fines diferentes al educativo (función docente y orientadora).
- El profesorado y resto del personal que acceda a los datos personales de los alumnos o de sus familias está sometido al deber de guardar secreto.

Los centros educativos también están legitimados para recabar datos sobre la situación familiar de los padres y/o tutores de los alumnos, que tienen la obligación de mantenerlos actualizados. Se establece que los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información necesaria sin la que no sería posible el desarrollo de la función educativa, estando los centros exceptuados de solicitar el consentimiento previo en relación a aquellos datos de carácter personal que sean necesarios para dicha finalidad. También deben facilitar los datos necesarios para el cumplimiento de la relación jurídica que se establece con la matrícula.

Asimismo, se pueden recabar datos sobre la salud del alumnado siempre que sean necesarios para el ejercicio de la función educativa. Se pueden distinguir los siguientes momentos:

- En la matriculación del alumno: discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias o alergias.
- Durante el curso escolar: el tratamiento médico que reciba un alumno a través del servicio médico o de enfermería del centro o los informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones sufridas en el centro o los informes de los equipos de orientación psicopedagógica.

B.1 ¿Pueden los centros hacer públicas las relaciones de los beneficiarios de becas, subvenciones y otras ayudas públicas?

La Ley de Transparencia y Acceso a la Información Pública y Buen Gobierno determina la obligación de hacer pública, como mínimo, la información relativa a las subvenciones y ayudas públicas concedidas por las Administraciones públicas con indicación de su importe, objetivo o finalidad y los beneficiarios.

Sin perjuicio de la publicación por parte de la Administración convocante, los centros escolares también podrán publicar esta información a efectos informativos de los afectados.

Cuando se trate de becas y ayudas fundadas en la situación de discapacidad de los beneficiarios será suficiente con publicar un listado con un número de identificación de los beneficiarios, como el del DNI o un número identificador que se hubiera facilitado a los interesados con la solicitud.

Así mismo, si fueran varios los requisitos a valorar, se podría dar el resultado total y no el parcial de cada uno de los requisitos. Si los criterios de las ayudas no se basan en circunstancias que impliquen el conocimiento de categorías especiales de datos hay que valorar si, no obstante, podrían afectar a la esfera íntima de la persona, por ejemplo al ponerse de manifiesto su capacidad económica o su situación de riesgo de exclusión social.

En estos casos habría que analizar en cada caso si resulta necesario hacer pública dicha información para garantizar la transparencia de la actividad relacionada con el funcionamiento y control de la actuación pública.

Igualmente, cuando ya no sean necesarios estos listados, habrá que retirarlos.

B.2 ¿Pueden los centros colocar en los tablones de anuncios o a las puertas de las aulas la relación de alumnos por clases y/o actividades?

Para la organización de la actividad docente los centros distribuyen al inicio de cada curso a los alumnos por clases, materias, actividades y servicios.

Para dar a conocer a los alumnos y a sus padres o tutores esta distribución, se pueden colocar dichas relaciones en los tablones de anuncios o en las entradas de las aulas, durante un tiempo razonable para permitir el conocimiento por todos los interesados.

Si el centro educativo utiliza una plataforma para la gestión educativa, se recomienda que cada alumno, sus padres o tutores accedan a dicha información mediante el uso de una identificación de usuario y su correspondiente contraseña.

B.3 ¿Pueden los profesores en prácticas utilizar datos personales de los alumnos para trabajos propios universitarios?

En la medida que no se estarían tratando los datos para la educación de los alumnos, sino para otra finalidad como la formación de los profesores, resulta aconsejable que procedan a disociar los datos de manera que no se puedan identificar a los alumnos. Si no, tendrán que contar con su consentimiento o el de sus padres o tutores si son menores de 14 años.

B.4 ¿Se pueden hacer públicas las calificaciones escolares?

Las calificaciones de los alumnos se han de facilitar a los propios alumnos y a sus padres. En el caso de comunicar las calificaciones a través de plataformas educativas, éstas sólo deberán estar accesibles para los propios alumnos, sus padres o tutores, sin que puedan tener acceso a las mismas personas distintas.
No obstante, sí sería posible comunicar la situación del alumno en el entorno de su clase, por ejemplo, mostrando su calificación frente a la media de sus compañeros.

B.5 ¿Pueden los profesores facilitar las calificaciones oralmente en clase?

Como se ha indicado, no existe una regulación respecto de la forma de comunicar las calificaciones. Aunque sería preferible que las calificaciones se notificasen en la forma indicada en el punto anterior, sería posible enunciarlas oralmente, evitando comentarios adicionales que pudieran afectar personalmente al alumno.

B.6 ¿Pueden los profesores acceder a los expedientes académicos de los alumnos matriculados en el centro?

Con carácter general y salvo que existiese alguna causa debidamente justificada, el profesor ha de tener acceso al expediente académico de los alumnos a los que imparte la docencia, sin que esté justificado acceder a los expedientes de los demás alumnos del centro.

Los profesores han de conocer y, por tanto, acceder a la información de salud de sus alumnos que sea necesaria para la impartición de la docencia, o para garantizar el adecuado cuidado del alumno, por ejemplo, respecto a discapacidades auditivas, físicas o psíquicas, trastornos de atención, TDAH o enfermedades crónicas. Igualmente, han de conocer la información relativa a las alergias, intolerancias alimentarias o la medicación que pudieran requerir para poder prestar el adecuado cuidado al alumno tanto en el propio centro como con ocasión de actividades fuera del centro, como visitas, excursiones o convivencias guiadas por profesores.

B.7 ¿Pueden los padres solicitar los exámenes de sus hijos para llevárselos ?

Esta cuestión no depende de la normativa de protección de datos, pues no se trata de un derecho de acceso a los datos, sino de acceso a documentación que, en su caso, deberá ser resuelta por el centro o la Administración educativa correspondiente con arreglo a su normativa interna y demás legislación sectorial que sea de aplicación.

En el caso del IES INGENIO, este procedimiento está recogido en el NOF del centro.

B.8 ¿Se puede facilitar la información escolar de los alumnos a sus familiares?

Sólo a los padres que ostenten la patria potestad o a los tutores legales, nunca a otros familiares, salvo que estuvieren autorizados por aquellos y constase claramente esa autorización.

B.9 Acceso a la información académica por padres separados

Toda la información relativa a estos casos se encuentra en la Resolución de 30 de junio de 2017, por la que se dictan instrucciones para la actuación de los centros docentes sostenidos con fondos públicos, en los casos de padres, madres, separados, divorciados, que hayan finalizado su convivencia, o representantes legales, respecto a sus descendientes o representados, menores de edad, en el ámbito de las enseñanzas no universitarias de la Comunidad Autónoma de Canarias.

B.10 ¿Se pueden comunicar los datos a las Fuerzas y Cuerpos de Seguridad?

Las comunicaciones de datos a las Fuerzas y Cuerpos de Seguridad son obligatorias siempre que sean necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

En todo caso, la petición que realicen las Fuerzas y Cuerpos de Seguridad, en el ejercicio de sus competencias, debe ser concreta, específica y motivada, de manera que no haya una comunicación de datos indiscriminada.

Aunque se cumplan los requisitos para la comunicación de datos a las Fuerzas y Cuerpos de Seguridad, es aconsejable que el centro documente la comunicación de los datos.

B.11 ¿Se pueden comunicar los datos a los Servicios Sociales?

Sí, siempre que sea para la determinación o tratamiento de situaciones de riesgo o desamparo competencia de los Servicios Sociales. La comunicación estaría amparada en el interés superior del menor, recogido en la Ley Orgánica de Protección Jurídica del Menor. En estos supuestos no se necesita el consentimiento de los interesados.

B.12 ¿En qué supuestos están los centros educativos obligados a comunicar datos de sus alumnos a las autoridades o sus agentes?

Cuando se tenga conocimiento de una posible situación de desprotección de un menor: de maltrato, de riesgo o de posible desamparo, se debe comunicar a la autoridad o a sus agentes más próximos.

También cuando se tenga conocimiento de la falta de asistencia de un menor al centro de forma habitual y sin justificación, durante el periodo lectivo, deberá trasladarse a la autoridad competente.

En estos casos no ha de mediar solicitud de ninguna autoridad o institución.

B.13 ¿Se pueden comunicar los datos a los centros sanitarios?

Se pueden facilitar los datos sin consentimiento de los interesados a los centros sanitarios cuando el motivo sea la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que se realicen por profesionales sanitarios sujetos al secreto profesional o por otras personas sujetas a la misma obligación.

Por ejemplo, cuando sea precisa la asistencia sanitaria a un alumno que se haya accidentado, indispuesto o intoxicado con la alimentación.

B.14 ¿Se pueden comunicar los datos a instituciones, entidades o empresas que van a ser visitadas por los alumnos en una actividad extraescolar, por ejemplo, una exposición, un museo, una fábrica o un club deportivo?

Sí, pero se debe contar con el consentimiento previo e inequívoco de los interesados o de sus padres o tutores, cuando los datos sean comunicados para las finalidades propias del teatro, museo, exposición o de la fábrica, por ejemplo, el control de entrada, de aforos o para sus programaciones futuras.

La información que sobre estos eventos se facilita a los padres para su autorización debe incluir la relativa a la comunicación de datos a estas entidades, así como la propia autorización. La comunicación, en caso de ser autorizada, implicaría la posibilidad del

tratamiento de los datos exclusivamente para los fines que se han indicado, al ser ésta necesaria para que el alumno pueda participar en esa actividad.

B.15 ¿Se pueden comunicar los datos de los alumnos y de sus padres y madres a las AMPA?

No sin el previo consentimiento de los interesados. Las AMPA son responsables del tratamiento de los datos de carácter personal que hayan recabado, debiendo cumplir con la normativa de protección de datos en su tratamiento.

No obstante, en el caso de que las AMPA fueran contratadas para prestar un servicio al centro educativo para el que tuvieran que tratar los datos de los alumnos y de sus padres sí tendrían acceso a los datos pero en condición de encargadas del tratamiento.

C. IMÁGENES Y VIDEOVIGILANCIA

Entre los datos que pueden recabar los centros educativos para el ejercicio de la función docente y orientadora sin consentimiento de los alumnos se pueden incluir sus fotografías a los efectos de identificar a cada alumno en relación con su expediente.

Con ocasión de la celebración de actos escolares o de eventos en centros educativos en los que los alumnos y los profesores son los protagonistas, tanto por los familiares como por el propio centro se toman fotografías y graban vídeos en los que se recogen sus imágenes. Estos hechos, comunes en los eventos escolares, dan lugar a que se planteen muchas cuestiones sobre quién y cómo se pueden captar las imágenes, qué requisitos se han de cumplir, con qué finalidad y a quién se pueden comunicar. Según quién vaya a grabar las imágenes y la finalidad para la que se graben será necesario observar unos determinados requisitos.

Si la grabación de las imágenes se produjera por el centro escolar con fines educativos, como trabajos escolares o evaluaciones, el centro o la Administración educativa estarían legitimados para dicho tratamiento sin necesidad del consentimiento de los alumnos o de sus padres o tutores. Cuando la grabación de las imágenes no se corresponda con dicha función educativa, sino que se trate de imágenes de acontecimientos o eventos que se graban habitualmente con fines de difusión en la revista escolar o en la web del centro, se necesitará contar con el consentimiento de los interesados, a quienes se habrá tenido que informar con anterioridad de la finalidad de la grabación, en especial de si las imágenes van a estar accesibles de manera indiscriminada o limitada a la comunidad escolar.

En caso de conflicto entre los progenitores sobre la grabación de las imágenes de sus hijos, deberá plantearse ante el juez competente en materia de familia para su resolución.

Por otra parte, es muy frecuente que los padres y familiares de alumnos tomen fotografías y graben vídeos en eventos festivos, conmemorativos, deportivos o de otra índole, en los que participan los alumnos.

En estos casos la grabación de las imágenes suele corresponder a una actividad exclusivamente personal y doméstica, es decir, aquellas que se inscriben en el marco de la vida privada, familiar y de amistad, que están excluidas de la aplicación de la normativa de protección de datos.

En otras ocasiones no es el centro escolar el que toma las fotografías o vídeos de los alumnos ni tampoco sus familiares, sino que son terceros, ya sea la empresa que presta un determinado servicio, por ejemplo, la celebración de actividades extraescolares o un club deportivo.

De nuevo hay que distinguir: si la grabación de imágenes se realiza por encargo del centro educativo, en cuyo caso éste deberá obtener el consentimiento de los alumnos o de sus padres o tutores, o si es el tercero quien toma la fotografías o graba los vídeos para sus propias finalidades, que tendrá que contar con el previo consentimiento de los interesados, ya lo recabe él mismo o a través del centro, en cuyo caso se deberá especificar que el tercero es el responsable del tratamiento

C.1 ¿Pueden los centros educativos captar imágenes de los alumnos durante las actividades escolares?

Cabría distinguir entre la toma de imágenes como parte de la función educativa, en cuyo caso los centros estarían legitimados para ello, de las grabaciones que no responderían a dicha función, por ejemplo, la difusión del centro y de sus actividades, para lo que se deberá disponer del consentimiento de los interesados o de sus padres o tutores.

También sería posible la toma de imágenes de los alumnos en determinados eventos desarrollados en el entorno escolar para la única finalidad de que los padres pudieran tener acceso a ellas. Este acceso a las imágenes debería siempre llevarse a cabo en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a las imágenes correspondientes a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso recordar a quienes acceden a las imágenes que no pueden, a su vez, proceder a su divulgación de forma abierta.

C.2 ¿Puede un profesor grabar imágenes de los alumnos para una actividad escolar?

Los profesores, en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados, pueden disponer la realización de ejercicios que impliquen la grabación de imágenes, normalmente de los propios alumnos, que sólo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente.

Es decir, en ningún caso el mero hecho de realizar la grabación supone que la misma se pueda difundir de forma abierta en Internet y que se pueda acceder de manera indiscriminada.

C.3 ¿Pueden los familiares de los alumnos que participan en un evento abierto a las familias grabar imágenes del evento?

Sí, siempre y cuando se trate de imágenes captadas exclusivamente para su uso personal y doméstico, pues en ese caso esta actividad está excluida de la aplicación de la normativa de protección de datos.

Si las imágenes captadas por los familiares se difundieran fuera del ámbito privado, familiar y de amistad, por ejemplo mediante su publicación en Internet accesible en abierto, los familiares asumirían la responsabilidad por la comunicación de las imágenes a terceros que no podrían realizar salvo que hubieran obtenido el consentimiento previo de los interesados.

Sería conveniente que el centro informase a los familiares de su responsabilidad en caso de que las imágenes fueran divulgadas en los entornos abiertos que acaban de señalarse.

C.4 Si unos padres se niegan a que se tomen imágenes de su hijo en un evento en el centro educativo, ¿se ha de cancelar dicho evento?

No. Se ha de informar a los padres que la toma de fotografías y vídeos es posible como actividad familiar, exclusivamente para uso personal y doméstico, que está excluida de la aplicación de la normativa de protección de datos.

C.5 ¿Y prohibir la toma de imágenes?

No, por los mismos motivos.

El IES INGENIO advertirá a los asistentes a los eventos organizados por el centro que se pueden grabar imágenes de los alumnos para su utilización exclusivamente personal, familiar y de amistad.
No se deben publicar este tipo de grabaciones en Internet en abierto, a no ser que se cuente con el consentimiento de todos aquellos que aparecen en las imágenes, de sus padres o tutores si son menores de 14 años.

C.6 La videovigilancia

La implantación de cámaras de videovigilancia, que responda al interés legítimo de los centros y de las Administraciones educativas en mantener la seguridad e integridad de personas y las instalaciones, ha de observar la normativa de protección de datos personales, en la medida que implica el tratamiento de los datos de alumnos, profesores, familiares, etc.

Dado el carácter intrusivo de estos sistemas en la intimidad de las personas, su instalación debe responder a los criterios de necesidad, idoneidad para los fines pretendidos, que no se puedan conseguir con una medida menos invasiva de la intimidad, y proporcionalidad, que ofrezca más beneficios que perjuicios. Por ejemplo, cuando el motivo para la instalación de estos sistemas sea el de evitar daños materiales, robos y hurtos que se pueden llegar a producir se podría limitar su funcionamiento a las horas no lectivas, de manera que se minimizara el impacto en la privacidad de las personas.

El RGPD establece varios supuestos en su artículo 6 que legitiman el tratamiento de datos de carácter personal, entre los que se encuentra permitir el tratamiento cuando sea necesario para el cumplimiento de una misión de interés público. Por lo tanto, y puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento. Asimismo, el considerando 45 del RGPD contempla que si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, este tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.

Registro de actividades: Videovigilancia

Responsable	Antonio Artiles Rodriguez
Actividad de tratamiento	Videovigilancia
Legitimación de tratamiento	Artículo 6.1. del RGPD: cumplimiento de una misión de interés público
Fines del tratamiento	Garantizar la seguridad de personas, bienes e instalaciones.
Delegado de Control de Datos	secretariaiesingenio@gmail.com IES INGENIO: 35010506 Avenida de los Artesanos, 55 Ingenio 35250 Islas Canarias. España; Teléfono: +34 928784600
Categoría de datos personales	Imagen
Categoría de afectados	Usuarios de las instalaciones. Personal docente, no docente, trabajadores del centro.
Descripción de las medidas técnicas y organizativas de seguridad	La grabadora de las cámaras está ubicada en un despacho perteneciente a un miembro del equipo directivo con acceso restringido. El acceso a las imágenes solo se realiza para la aclaración de algún hecho acaecido en el centro o que pueda constituir un acto delictivo .
Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales	Fuerzas y Cuerpos de Seguridad del Estado. Juzgados y Tribunales.
Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1	No existen (como regla general)
Cuando sea posible, plazo para la supresión de las diferentes categorías de datos	Transcurridos 10 días se sobreescriben las imágenes excepto si son extraídas para su uso por las fuerzas y cuerpos de Seguridad del Estado así como juzgados y tribunales.

Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, es decir, la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, el responsable del tratamiento que sufra dicha brecha, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo a la AEPD, en un plazo máximo de 72 horas.

El contenido mínimo de la comunicación de la brecha de seguridad a la AEPD será:

- naturaleza de la brecha de seguridad: categorías de afectados (pj. menores, discapacitados, empleados, ciudadanos)
- número aproximado de afectados
- categorías de datos comprometidos (pj. identificativos, salud, laborales)
- número de registros de datos personales afectados

En todo caso deberán tenerse en cuenta las siguientes indicaciones:

- La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.
- No podrán instalarse en espacios protegidos por el derecho a la intimidad como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada como los gimnasios.
- Salvo en circunstancias excepcionales, no podrán utilizarse con fines de control de asistencia escolar.
- Se pueden instalar cámaras en los patios de recreo y comedores cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.
- La grabación en las aulas mientras los alumnos realizan pruebas de nivel de conocimientos sería desproporcionado.

C.7 ¿Se pueden instalar cámaras de videovigilancia en las aulas alegando motivos de conflictividad?

Resultaría desproporcionado, pues durante las clases ya está presente un profesor. Además de una intromisión en la privacidad de los alumnos, podría suponer un control laboral desproporcionado de los profesores.

Cabría la posibilidad de que, fuera del horario lectivo y en los supuestos de desocupación de las aulas, se pudieran activar mecanismos de videovigilancia con la finalidad de protección a los alumnos y de evitar daños en las instalaciones y materiales.

C.8 ¿Se pueden instalar cámaras de videovigilancia en los patios de recreo y pasillos?

Sí, cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.

D. TRATAMIENTO DE DATOS EN INTERNET

La mayoría de los Centros permite la utilización de estas aplicaciones, declarando en muchos casos que mediante ellas se almacenan datos personales, si bien normalmente limitados al nombre y apellidos de los alumnos. También se almacenan trabajos realizados y, en menor medida, calificaciones. Asimismo, se ha declarado el almacenamiento de fotos, videos y grabaciones de voz.

Las aplicaciones utilizadas responden a una gran variedad, que se pueden clasificar en los siguientes tipos según su funcionalidad (se mencionan entre paréntesis algunas aplicaciones a modo de ejemplo):

1. Aplicaciones que implementan cuadernos de notas, agendas y organizador de clases para los docentes (IDOCEO, ADDITIO, TEACHER AIDE).

2. Aplicaciones puramente destinadas a ofrecer materiales didácticos atrayentes para los alumnos y de utilidad para los profesores, de diferentes materias como matemáticas, ciencias, (DIDAKIDS), incluyendo gamificación (CLASSCRAFT, KAHOOT), etc.

3. Aplicaciones para la creación de hilos de discusión y debate, compartición de mapas mentales, conceptuales y esquemas (MINDOMO).

4. Aplicaciones para la elaboración de presentaciones (PREZI, TED).

5. Aplicaciones que facilitan la comunicación entre profesores, alumnos y familias. Si bien esta funcionalidad se suele incorporar en las plataformas educativas, existen apps con esta finalidad exclusiva. También, dentro de este tipo de aplicaciones, señalar que se ha detectado la utilización de mensajería WHATSAPP en los entornos educativos.

6. Creación y compartición de vídeos. (ANIMOTO, MOVIE MAKER). Edición y compartición de fotografías y vídeos (PicCOLLAGE).

7. Aplicaciones que convierten tabletas en pizarras digitales para compartir información en tiempo real (ACTIVEINSPIRE).

8. Apps para el acceso desde el terminal móvil a plataformas de aprendizaje (MOODLE, LMS WORDPRESS, SCHOOLOGY), para la compartición de recursos de estudio, realización de trabajos en grupo, etc. También existen redes sociales educativas con funciones de plataformas de aprendizaje (CLASSROOM, EDMODO).

Las aplicaciones que más datos personales de los alumnos pueden llegar a tratar son los cuadernos de notas de los docentes, que mantienen el progreso y las calificaciones de los alumnos, sin olvidar que aunque la mayoría del resto de aplicaciones no recopilan

datos personales más allá de los básicos de usuario, cualquier aplicación que incluya la identificación del alumno puede llevar a la elaboración de perfiles según las funcionalidades y la tipología de los datos recopilados.

Hay que tener en cuenta que las aplicaciones instalables en dispositivos móviles inteligentes son capaces de acceder a gran cantidad de datos de carácter personal almacenados en el propio dispositivo, tales como el número de identificación del terminal, agenda de contactos, imágenes o vídeos. Además, estas aplicaciones pueden acceder a los sensores del dispositivo, y obtener la ubicación geográfica, capturar fotos, vídeo o sonido a través de ellos.

Los Centros Educativos deben observar la debida diligencia con los tratamientos de datos personales que se efectúen en el Centro, incluyendo los que se producen como consecuencia de la llegada de las tecnologías a las aulas, velando por que se reúnan las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos.

Algunas aplicaciones utilizadas no ofrecen suficiente información para valorar su adecuación a la normativa. Por ejemplo, en materia de seguridad, sobre la ubicación de los datos, el periodo de retención de los mismos, ni los responsables de los tratamientos. En ocasiones no incluyen información ni tan siquiera sobre las finalidades de los tratamientos, detectándose falta de transparencia y la posibilidad de prácticas de retención de datos opacas.

Dadas las funcionalidades que ofrecen estas aplicaciones y la tipología de los datos que tratan, los tratamientos efectuados podrían incluir la elaboración de perfiles de aprendizaje, preferencias o comportamiento de menores de edad, por parte de los responsables de las aplicaciones.

Por ello, deben utilizarse únicamente aquellas aplicaciones que ofrezcan información claramente definida sobre los tratamientos efectuados, las finalidades de los mismos y sus responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad.

Las aplicaciones educativas, que pueden ser de gran utilidad para el aprendizaje así como para la organización de las aulas, deben estar incluidas en la política de seguridad de los centros educativos, debiendo los profesores solicitar, previamente a su utilización, la autorización del centro.

Deben establecerse procedimientos que obliguen a solicitar la autorización del Centro para el uso de estas aplicaciones. Una solicitud de autorización conllevará la evaluación de la aplicación desde el punto de vista de la seguridad de la información y la consiguiente autorización o denegación por parte del Centro.

Los tratamientos de datos personales mediante apps deben de incluirse en la política de seguridad con las mismas garantías que cualquier otro tratamiento.

D.1. Evaluación de las aplicaciones que se utilizarán

Para la evaluación de las aplicaciones desde el punto de vista de la protección de los datos personales y la seguridad de la información el profesorado del IES INGENIO deberá seguir las siguientes orientaciones:

a) Sobre la información ofrecida por los responsables de la aplicación:

• La identidad y dirección del responsable,
• Las finalidades para las que serán utilizados los datos,
• Las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad por la que se ceden,
• Los derechos que asisten a los titulares de los datos,
• La ubicación de los datos y sus periodos de conservación,
• Las medidas de seguridad facilitadas por la aplicación,
• Los posibles accesos que realiza la aplicación a los datos personales almacenados en el dispositivo o a sus sensores.

Esta información debería estar fácilmente accesible en la política de seguridad de la aplicación. En caso de que falte alguno de estos aspectos, o que la información facilitada no ofrezca las garantías adecuadas, se recomienda no utilizar la aplicación.

b) Sobre la ubicación de los datos:

Los datos deben estar almacenados en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea).

c) Sobre la seguridad de los datos:

La aplicación debe proveer mecanismos que permitan la realización de copias de seguridad o la descarga de los datos, de tal forma que el Centro pueda cumplir con las obligaciones que le son exigibles al respecto, introduciendo en su política de seguridad la realización de copias de seguridad de los datos tratados mediante estas aplicaciones, y realizando efectivamente la realización de dichas copias.

La responsabilidad de las medidas de identificación de usuarios también es compartida. Por un lado, la aplicación debe implementar un mecanismo de autenticación

que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas.

d) Prueba de la aplicación:

Se considera conveniente poner a prueba la aplicación de forma previa a su definitiva utilización en el Centro, realizando la prueba sin introducir datos personales reales de los alumnos ni involucrarlos en su utilización. En esta fase de prueba se debería comprobar la
corrección de las informaciones que fueron facilitadas por el responsable de la aplicación.

e) Documentación de la evaluación:

Se recomienda documentar las evaluaciones realizadas dejando constancia de los aspectos que han sido analizados y de los resultados obtenidos.

D.2 ¿Se pueden publicar en la web del centro los datos de los profesores, tutores y otros responsables del centro?

Si se trata de una web en abierto, sería necesario contar con su consentimiento previo dado que se trata de una comunicación de datos a los que puede acceder cualquier persona de manera indiscriminada y no resulta necesaria para el ejercicio de la función educativa encomendada a los centros.

D.3 ¿Puede publicarse en la web del centro información relativa a los alumnos, como fotografías o vídeos?

Sí, siempre que se disponga del consentimiento de los alumnos o de sus padres o tutores. También podría llevarse a cabo de manera que no se pudiera identificar a los alumnos, por ejemplo, pixelando las imágenes.

También sería posible su publicación cuando responda a determinados eventos desarrollados en el entorno escolar con la única finalidad de que los padres pudieran tener acceso a ella. Este acceso debería llevarse a cabo siempre en un entorno seguro que exigiera la previa identificación y autenticación de los alumnos, padres o tutores (por ejemplo, en un área restringida de la intranet del centro), limitándose a la información correspondiente a eventos en los que el alumno concreto hubiera participado. En todo caso, sería preciso recordar a quienes acceden a la información que no pueden, a su vez, proceder a su divulgación de forma abierta y que no pueden proceder a su divulgación

D.4 ¿Pueden publicarse datos personales de los alumnos en el blog del centro educativo?

Como en el caso de la web, si el contenido del blog en abierto del centro educativo incluyera datos que permitieran la identificación de los alumnos, se requeriría su consentimiento o el de sus padres o tutores.

En estos casos se aconseja disociar o anonimizar los datos de los alumnos, de manera que no se les pueda identificar.

D.5 ¿Y un profesor puede publicar en su blog las actas del departamento o los exámenes de los alumnos o sus fotografías?

El blog de un profesor es un medio de información y comunicación al margen de la función docente que desarrolla en los centros educativos. De su contenido será responsable el profesor que deberá observar la normativa de protección de datos en cuanto que incluya información de carácter personal.

Por tanto, salvo que se contase con el consentimiento de los afectados, o de sus padres o tutores, no se podrían publicar en el blog de un profesor datos de carácter personal que permitan identificar a los alumnos.

Al igual que con los blogs de los centros educativos, se podría publicar la información previa disociación o anonimización de los datos de los alumnos de manera que no se les pudiese llegar a identificar.

D.6 ¿Pueden los profesores crear grupos con aplicaciones de mensajería instantánea con el alumnado?

Con carácter general, las comunicaciones entre los profesores y los alumnos deben tener lugar dentro del ámbito de la función educativa y no llevarse a cabo a través de aplicaciones de mensajería instantánea.

En situaciones concretas, como la realización de una tarea, un trabajo específico, un viaje y otras situaciones valoradas por el profesorado junto al equipo directivo y a las familias, se podrían crear con carácter excepcional, siendo aconsejable la participación en el grupo de un tercero, padre o madre de los alumnos.

E. CESIÓN DE DATOS

Siempre que los datos personales se envían fuera del ámbito de Espacio Económico Europeo (EEE), que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos, ya se realice para que el destinatario *de los datos preste un servicio al centro educativo o para que los trate para una finalidad propia.*

Se realizan transferencias internacionales de datos cuando se contratan servicios de *cloud computing* en los que, por ejemplo, el alojamiento de datos se realiza en servidores fuera del EEE, o cuando se comunican a centros educativos establecidos en países fuera de este ámbito para realizar intercambios de alumnos o periodos de formación.

No son transferencias internacionales de datos las que se realicen con destino a Estados de la Unión Europea o del EEE, aunque dichas transmisiones deberán cumplir los requisitos establecidos por la Ley para la validez de las cesiones de datos o la contratación de un encargado del tratamiento.

No se cederán datos a terceros excepto en el cumplimiento de las obligaciones legales establecidas en el seno de la cooperación entre administraciones.

F. LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS

Además del consentimiento, existen otras posibles bases que legitiman el tratamiento de datos sin necesidad de contar con la autorización de su titular. La principal de ellas es la referida a los supuestos en que una norma con rango de Ley autorice el tratamiento o incluso obligue al responsable a llevarlo a cabo.

También será legítimo el tratamiento de datos cuando sea necesario para el desarrollo y ejecución de una relación jurídica entre el responsable y el afectado, o para la satisfacción de un interés legítimo del responsable siempre que dicho interés no prevalezca sobre los derechos y libertades de los afectados, en particular cuando éstos sean niños.

Los centros docentes están legitimados por la Ley Orgánica de Educación de 2006 (LOE) para el tratamiento de los datos en el ejercicio de la función educativa. También están legitimados para el desarrollo y ejecución de la relación jurídica que se produce con la matriculación del alumno en un centro, así como por el consentimiento de los interesados, o de sus padres o tutores si son menores de 14 años, o por la existencia en los centros privados de intereses legítimos que, previa ponderación con los derechos y libertades de los afectados, se considere que prevalecen sobre éstos. También se legitima a través de la Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa (LOMCE).

Si se recogieron datos para realizar la matrícula, no se podrán utilizar para finalidades diferentes del ejercicio de la función educativa, como la publicación de fotografías de los alumnos en la web del centro o la comunicación de sus datos a museos o empresas para organizar visitas, salvo que se haya recabado el consentimiento de los alumnos o de sus padres o tutores tras haberles informado de ello.

G. INFORMACIÓN

Cuando se recaban o se obtienen los datos de los interesados, aun cuando no sea necesario su consentimiento, el IES Ingenio les facilitará, en sus impresos, información de los siguientes extremos:

- de la existencia de un fichero o tratamiento de datos personales,
- de la finalidad para la que se recaban los datos y su licitud, por ejemplo, para el ejercicio de la función educativa, o para difundir y dar a conocer las actividades del centro,
- de la obligatoriedad o no de facilitar los datos y de las consecuencias de negarse,
- de los destinatarios de los datos,
- de los derechos de los interesados y dónde ejercitarlos,
- de la identidad del responsable del tratamiento: el centro o la Administración educativa.

H. MEDIDAS DE SEGURIDAD

Los centros y las Administraciones educativas, como responsables de los tratamientos de datos personales que realizan, deben adoptar una serie de medidas de seguridad, de carácter técnico y organizativo, que garanticen la seguridad de los citados datos, es decir, su integridad y confidencialidad y la protección frente al tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

En la actualidad, el Reglamento de desarrollo de la LOPD, en su Título VIII, configura un catálogo de medidas de seguridad en tres niveles (básico, medio y alto) en función del tipo de datos, de quién sea el responsable del tratamiento y de la finalidad para la que se traten.

Además, las Administraciones educativas deberán cumplir, en su caso, con los principios básicos y requisitos mínimos que permitan una protección adecuada de la información de conformidad con lo establecido en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica).

Los centros y las Administraciones educativas, como responsables del tratamiento, tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratar dichos datos en el ejercicio de las funciones que tenga asignadas.

Con el objetivo de salvaguardar la seguridad de los datos personales, el IES INGENIO ha adoptado todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales suministrados. Todo ello para evitar su alteración, pérdida, y/o tratamientos o accesos no autorizados, tal como exige la normativa, si bien la seguridad absoluta no existe.

Igualmente, el IES INGENIO informa que todo nuestro personal, cualquiera que sea la fase del tratamiento en la que intervenga, adoptará el compromiso de tratar sus datos personales con el máximo cuidado y confidencialidad y que su tratamiento se efectuará de acuerdo con la legislación vigente sobre protección de datos de carácter personal, en particular con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Le recordamos que ni el IES INGENIO, ni cualquiera de sus empleados, cederá o comunicará ningún dato a terceros, excepto en los casos legalmente previstos, o salvo que se le autorice expresamente.

El momento en que se detecta e identifica una brecha de seguridad es importante ya que el RGPD establece que el responsable del tratamiento debe notificarlo a la autoridad de control competente sin dilación indebida y, de ser posible, en un plazo máximo de 72 horas después de que haya tenido constancia de ella. En determinados casos se deberá notificar también a los afectados.

Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas, como por ejemplo:

1 Políticas específicas de mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, etc.

2 Controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a determinadas zonas, etc.

3 Controles y procedimientos frente a daños ambientales o desastres naturales. En este sentido, cobra suma importancia la concienciación y formación de todo el personal de la organización para evitar situaciones de riesgo e incluso detectarlas y notificarlas.

En cuanto a los controles de ciberseguridad, atendiendo a las características particulares de la organización, se puede contar con medios manuales, como la notificación de problemas por parte del personal de la organización, y sistemas automatizados de detección de diferentes tipos, desde software antivirus hasta analizadores de logos.

Es preciso tener en cuenta que con frecuencia un incidente que tenga lugar en el ámbito de la seguridad física puede también tener repercusión en el contexto de la ciberseguridad y por lo tanto en los tratamientos de datos personales, de ahí la necesidad de mantener cierto grado de coordinación entre los responsables de la seguridad física y la ciberseguridad. Será la Consejería de Educación, propietaria de todos los programas que se utilizan por los centros educativos, la responsable de mantener informados a los mismos de cualquier vulnerabilidad. Al IES INGENIO le corresponderá informar de cualquier ataque a su página web o a su moodle.

Sin ánimo de exhaustividad, se pueden considerar las siguientes fuentes de información:

1. Notificaciones de usuarios: presencia de archivos con caracteres inusuales, recepción de correos electrónicos con archivos adjuntos sospechosos, comportamiento extraño de dispositivos, imposibilidad de acceder a ciertos servicios, extravío/robo de dispositivos de almacenamiento o equipos con información.
2. Alertas generadas por software antivirus.
3. Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
4. Anomalías de tráfico de red o picos de tráfico en horas inusuales.
5. Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).
6. Alertas de sistemas de correlación de eventos.
7. Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.
8. Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
9. Análisis de registros en herramientas DLP (Data Loss Prevention).

I. DEBER DE SECRETO

Todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre los mismos.

Este deber de secreto es esencial para garantizar el derecho fundamental a la protección de datos y es de obligado cumplimiento para todas las personas que presten sus servicios en los centros y Administraciones educativas -docentes, personal administrativo o de servicios auxiliares-, en relación con los datos de carácter personal a los que accedan.

Además, el deber de secreto subsiste incluso una vez finaliza la relación con el responsable o con el encargado de tratamiento.

J. DERECHOS DE LOS USUARIOS

Estos derechos son los de acceso, rectificación, cancelación y oposición, conocidos por su acrónimo ARCO, y se pueden describir del siguiente modo:

A) ACCESO

El derecho de ACCESO permite a los titulares de los datos personales conocer y obtener gratuitamente información sobre si sus datos de carácter personal están siendo objeto de tratamiento, con qué finalidad, qué tipo de datos tiene el responsable del tratamiento, su origen, si no proceden de los interesados, y los destinatarios de los datos.

El derecho de acceso a los datos personales es independiente del derecho de acceso al expediente, a la información y documentación, que se rigen por otra normativa. Conforme a la normativa de protección de datos, no hay obligación de facilitar copia del expediente escolar, sin perjuicio del acceso a la información en el marco de la legislación sectorial.

B) RECTIFICACIÓN

El derecho de RECTIFICACIÓN permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Este derecho de rectificación no se aplica a las calificaciones o al contenido de los informes del expediente escolar que se rigen por su normativa específica.

No puede ejercitarse el derecho de rectificación para modificar un informe de evaluación psicopedagógica ya que no se puede tratar de modificar la opinión realizada por un profesional a través del correspondiente informe que se rige por su normativa específica.

C) CANCELACIÓN

El derecho de CANCELACIÓN permite que se supriman los datos que resulten ser inadecuados o excesivos. La revocación del consentimiento da lugar a la cancelación de los datos cuando su tratamiento esté basado en él.

Como regla general, se conservarán por el tiempo estrictamente necesario para las finalidades para las que se recabaron y para hacer frente a las responsabilidades que se pudieran derivar de su tratamiento, de manera que cuando hayan dejado de ser necesarios o pertinentes para dicha finalidad deberá producirse la cancelación de los mismos.

La cancelación da lugar al bloqueo de los datos, que no implica su borrado material sino su identificación con la finalidad de impedir su ulterior proceso o utilización, excepto para ponerlos a disposición únicamente de las Administraciones públicas, Jueces y Tribunales para la determinación de posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de éstas, limitándose en este caso el acceso a personas con la máxima responsabilidad. Cumplido dicho plazo debe procederse a su destrucción, para lo que se deberán utilizar medios que aseguren que no puedan acceder a los datos terceros no autorizados.

El tiempo que se deben conservar los datos será el que establezcan las disposiciones aplicables o, en su caso, las relaciones contractuales entre los interesados y los centros educativos. Dada la pluralidad de ficheros y finalidades para las que se recaban y tratan los datos, no se puede establecer un determinado plazo, si bien deberán mantenerse en cuanto que puedan ser necesarios para el ejercicio de alguna acción por parte de los alumnos, por lo que resultaría preciso definir el alcance de las responsabilidades de los centros educativos en relación con el contenido y custodia de los datos.

D) OPOSICIÓN

El derecho de OPOSICIÓN es el derecho del interesado a que, por motivos relacionados con su situación personal, no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

La familia puede ejercer este derecho cuando exista un motivo legítimo y fundado, referido a una concreta situación personal, para oponerse a la publicidad de su información personal. Por ejemplo, en los casos en los que se ha acordado por los jueces el alejamiento de uno de los progenitores o se le ha privado de la patria potestad y la publicidad de información personal pueda suponer un riesgo para la integridad física y psíquica del alumno o del otro progenitor.

J.1 ¿Quiénes pueden ejercitar estos derechos?

Estos derechos tienen carácter personalísimo, lo que significa que sólo pueden ser ejercidos por sus titulares o sus representantes legales. En el caso de los menores de 14 años, los padres, cuando ostenten la patria potestad, o los tutores podrán ejercitarlos en su nombre. Si son mayores de esa edad lo podrán ejercitar los propios alumnos o sus representantes legales, que igualmente pueden ser sus padres.

Si se trata de los datos de los padres serán éstos los legitimados para ejercitarlos.

ANEXO I: VERIFICACIÓN DE LAS CONDICIONES DE CONSENTIMIENTO

Este listado de verificación deberá tenerse en cuenta en la información de realización de cualquier tipo de actividad que precise el consentimiento de los tutores legales del alumnado.

CONDICIONES PARA EL CONSENTIMIENTO	
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal Se solicita el consentimiento de forma clara e independiente de los demás asuntos	
Se solicita el consentimiento de forma inteligible y de fácil acceso	
Se solicita usando lenguaje claro y sencillo Se informa con carácter previo a recabar el consentimiento Se permite retirar el consentimiento con la misma facilidad que se recaba Se recaba el libre consentimiento	
Para prestar un servicio se solicitan sólo los datos necesarios	

ANEXO II: VERIFICACIÓN DE TRANSFERENCIAS DE DATOS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES

TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES	
Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de nivel de protección adecuado por la Comisión Europea	
Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea	
Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales.	
Existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos	
Existen normas corporativas vinculantes	
Existen cláusulas tipo de protección de datos adoptadas por la Comisión	
Existen cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión	
Existe un código de conducta junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existe un mecanismo de certificación junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existen cláusulas contractuales que requieren la autorización previa de la autoridad de control	
Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados	
Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas	
Se dispone del consentimiento explícito del interesados y se le ha informado de los posibles riesgos	
Son necesarias para la ejecución de un contrato con el interesado o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado	
Son necesarias para la formulación, ejercicio o la defensa de reclamaciones	
Son necesarias para la protección de los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento	
Se dispone del consentimiento explícito del interesados y se le ha informado de los posibles	
Por intereses legítimos imperiosos	
Afecta a un número limitado de interesados y no es repetitiva	
Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantías apropiadas	
Se ha informado a la autoridad de control	

ANEXO III: SOLICITUD DE UTILIZACIÓN DE APLICACIONES EDUCATIVAS

Protocolo de Protección de Datos

DATOS SOLICITANTE

Apellidos y nombre:
Departamento:
Aplicación educativa que se solicita:
Uso: ☐ individual ☐ todos los miembros del departamento

DATOS APLICACIÓN

El responsable de la aplicación informa:	
la identidad y dirección del responsable	
las finalidades para las que serán utilizados los datos	
las posibles comunicaciones de datos a terceros y su identidad, así como la finalidad por la que se ceden	
los derechos que asisten a los titulares de los datos	
la ubicación de los datos y sus periodos de conservación	
las medidas de seguridad facilitadas por la aplicación	
los posibles accesos que realiza la aplicación a los datos personales	
almacenados en el dispositivo o a sus sensores	
Los datos deben estar almacenados en un país del Espacio Económico Europeo o un país que ofrezca un nivel de protección equivalente (que haya sido así acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea).	
Se utilizará:	
Datos del alumnado	
Imágenes del alumnado	
Videos donde aparezca el alumnado	
Contraseñas de acceso	
Almacenamiento de datos en la nube	
Uso de teléfonos inteligentes	
Plataformas educativas	
Redes sociales	
Correos electrónicos del alumnado	
Otros:	

Protocolo de Protección de Datos

JUSTIFICACIÓN DE UTILIZACIÓN

Materia:
Temporalización del uso de la aplicación:
Justificación didáctica:
Criterios y estándares de aprendizaje que justifican el uso de la aplicación:
Instrumentos de evaluación de la/s actividad/es donde se utilizará la aplicación:
Observaciones:

Se solicita la autorización de la dirección del centro para el uso de la aplicación que se explicita en los datos aportados, aceptando el deber de aplicar las políticas de privacidad de datos y las de seguridad del tratamiento de los mismos, ejerciendo el control del uso de las aplicaciones para el uso específico que se solicita.

En la Villa de Ingenio, a de de

Fdo:

Se informa que el presente documento, una vez autorizado el uso de la aplicación, implica que el/la profesor/a debe garantizar el cumplimiento específico de las condiciones de uso, siendo responsable de cualquier uso negligente del mismo bajo su control.