PROTOCOLO PROTECCIÓN DE DATOS

C.E.I.P. Miguel de Cervantes

ÍNDICE

INTRODUCCIÓN Y JUSTIFICACIÓN DEL PROTOCOLO

El C.E.I.P. “Miguel de Cervantes” se encuentra en la localidad de Lucena del Puerto, municipio de la provincia de Huelva, situado en la zona sur occidental de la cuenca del Guadalquivir, en la orilla izquierda del río Tinto, en entorno Doñana.

Lucena del Puerto tiene una población de unos 3187 habitantes (año 2021 (más del 70% de ella se dedica a la agricultura), aunque el número de habitantes aumenta considerablemente en la época de plantación y recolección de la fresa, fresón, frambuesas y arándanos con población desplazada temporalmente, llegándose a duplicar la población.

El colegio se encuentra en un extremo del pueblo y está dividido en tres bloques: El bloque I está ocupado por cuatro aulas de alumnos/as de Educación Secundaria, dos aulas de Educación Primaria, Biblioteca, aula de A.T.A.L y aula de Pedagogía Terapéutica, además de la sala de profesores y despachos de administración. La edad del alumnado que en él se encuentran, oscila entre los 12 y 15 años; el bloque II está ocupado por el aula de informática y por alumnos/as de Educación Primaria, de 3º a 5º, con edades comprendidas entre los 8 y 10 años y el bloque III está ocupado por alumnos/as del 2º Ciclo de Educación Infantil, en su planta baja, y por alumnos/as del 1º ciclo de Educación Primaria. Sus edades oscilan entre los tres y siete años. Entre los bloques I, II y III, separándolos una larga escalera, se ubican el SUM, comedor, gimnasio, invernadero y pista polideportiva.

El horario general del Centro es un poco complicado porque hay que conjugar varias circunstancias: el aula matinal, transporte escolar de los alumnos desplazados, comedor, horarios diferentes en Infantil-Primaria y ESO, el tiempo de recreo, cierto profesorado también compartido… Así, tenemos como horario en E.S.O de 8:00 a 14.30, con el recreo de 11:00 a 11:30 y en Infantil- Primaria de 9:00 a 14:00, con el recreo de 12:00 a 12:30.

Respecto a la comunidad educativa, el centro cuenta con alumnos desplazados, "temporeros" (procedentes fundamentalmente de la zona de Cádiz), pero ahora, al igual que la mayoría de pueblos freseros, son mayoritarios los inmigrantes, conviviendo en el colegio 5 nacionalidades (española, ghanesa, rumana, marroquí y polaca).

La población local podríamos decir que goza de un estatus socio- económico medio-alto, pero existe una significativa minoría que no alcanza un nivel mínimo aceptable; más baja se considera la media si nos referimos al factor cultural. Entre la comunidad existe un bajo nivel de motivación e interés hacia los estudios ya que han canalizado su futuro hacia las tareas agrícolas u otras que se puedan dar en el pueblo,

aunque poco a poco se va imponiendo la motivación hacia estudios universitarios con diferentes salidas laborales.

En el curso 2015/2016 volvió a constituirse la AMPA, preocupada por colaborar en la vida escolar del alumnado, motivando a las familias en la participación tanto de actividades como en el seguimiento académico de sus hijos/as, siendo la familia pieza fundamental para el buen desarrollo académico.

Cada vez más, tanto en el desarrollo de las actividades académicas, las complementarias, el seguimiento escolar, las consultas con las familias, las informaciones compartidas... se realiza con equipos tecnológicos e internet como herramienta imprescindible, adjudicándole una importancia real a la protección de datos que podemos compartir entre el triángulo formado por maestros-alumnos-familias siendo éste el motivo y la justificación de la elaboración de este Protocolo.

MARCO NORMATIVO REFERENTE A PROTECCIÓN DE DATOS

Para la Protección de datos es fundamental atender a la legislación y normativa aplicable:

- Reglamento General de Protección de Datos 2016/679, de 27 de abril de 2016, aprobado por el Parlamento Europeo y el Consejo de la Unión Europea, y que regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea. El fundamento principal y el espíritu de la norma se centra en la necesidad de regular el impacto de la tecnología, el progresivo tratamiento de datos en soporte informatizado o el crecimiento en las capacidades de almacenamiento de datos.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, aprobada por las Cortes Generales de España. Su finalidad es proteger la intimidad, privacidad e integridad del individuo, en cumplimiento con el artículo 18.4 de la Constitución Española, del mismo modo, regula las obligaciones del individuo en todo proceso de transferencia de datos para garantizar la seguridad del intercambio. Además, otra de sus principales finalidades es establecer un marco legislativo para la protección de datos personales en Internet.

Un centro educativo presenta peculiaridades a la hora de tratar datos, es por ello que se aprueban otras normas complementarias. Se pueden consultar algunas de ellas en el siguiente enlace: Normativa complementaria de Protección de Datos.

Es interesante destacar que la Agencia Española de Protección de Datos ha publicado una Guía que incluye los conceptos y principios básicos en materia de

protección de datos que pretende facilitar la aplicación concreta a las situaciones que se presentan en la práctica teniendo presente la perspectiva del nuevo Reglamento General de Protección de Datos. Ver Guía.

Además de la normativa señalada, es importante considerar el Código de Uso de TIC por parte del personal al servicio de la Junta de Andalucía, en este caso los docentes.

CONCEPTOS BÁSICOS

· Responsable del tratamiento de datos: 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. En nuestro centro educativo será responsable del tratamiento la Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía.

· Persona encargada del tratamiento: persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento. Es el propio centro educativo quien ostenta esta figura. Debiendo ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas que lleven al cumplimiento real y efectivo de la normativa vigente de protección de datos y garantizar la protección de los derechos del interesado, como indica el artículo 28 del Reglamento de Protección de Datos.

· Principio de Responsabilidad Proactiva: El responsable del tratamiento y el centro educativo debe garantizar y poder demostrar, ante la autoridad y las personas interesadas, que el tratamiento es conforme a la normativa de protección de datos y que ha adoptado las medidas más adecuadas para garantizar los derechos y las libertades de las personas de las que se tratan datos. Este principio require que el centro educativo analice qué datos trata, con qué fines lo hace y qué tipo de operaciones de tratamiento lleva a cabo. A partir de este conocimiento detallado, debe valorar el riesgo que puede generar este tratamiento y, de acuerdo con esta valoración, adoptar las medidas de seguridad pertinentes.

· Delegado de Protección de Datos: Según la Agencia Española de Protección de Datos, el centro “está obligado a designar un delegado de protección de datos en los supuestos recogidos en el artículo 37 del Reglamento General de Protección de Datos y, en todo caso, cuando ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas, conforme lo estipula el artículo 34.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”. Por tanto,

nuestro centro, al impartir enseñanzas en Infantil, Primaria y ESO, está obligado a designar un delegado de protección de datos.

· Obligación de informar: El colegio tiene la obligación de informar en los términos legales del tratamiento que realiza legitimado por una norma por rango legal, así como recabar el consentimiento para los tratamientos que lo requieran utilizando un modelo ajustado a la legalidad vigente y conservando los medios probatorios de la prestación del consentimiento informado. Se tratarán datos de carácter personal del alumnado y de sus familiares con la debida diligencia y respeto a su privacidad e intimidad, teniendo presente el interés y la protección de los menores. Se deberá implementar un plan de información y formación que permita y promueva el respeto y el cumplimiento de la normativa vigente por parte de las personas encargadas del tratamiento de datos en el desarrollo de sus funciones en la organización.

· Política de protección de datos: En el colegio es imprescindible establecer un conjunto de reglas y procedimientos vigentes y aplicables dentro del ámbito de autoridad de una organización, es decir, que estas políticas de protección de datos están dirigidas a las personas que tienen acceso y utilizan datos personales, con el fin de garantizar la seguridad de esta información. La obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado corresponde tanto al responsable como al encargado del tratamiento de los datos.

· Datos personales: Toda información sobre una persona física identificada o identificable, entendiéndose por identificable a aquellos supuestos en los que pueda determinarse la identidad de una persona, 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. (P. ej: nombres y apellidos del alumnado o de sus familiares, su dirección, su número de teléfono o su correo electrónico, las imágenes del alumnado o, por ejemplo, la profesión, los estudios o el lugar donde trabajan los familiares, o su número de cuenta bancaria).

Señalar que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

· Datos de carácter sensible: Aquellas circunstancias o información de las personas que se refieren a su esfera más íntima y personal, por ejemplo concernientes a la

ideología, afiliación sindical, religión y creencias origen racial, a la salud y a la vida sexual, o aquellos que se refieran a la comisión de infracciones penales o administrativas, datos biométricos y genéticos. Las excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales deben establecerse de forma explícita cuando el interesado dé su consentimiento explícito o concurran determinadas razones vinculadas al interés público, razones sanitarias, de seguridad, o cuando sea necesario para permitir el ejercicio de libertad fundamentales por razones de interés público. En el colegio podemos realizar el tratamiento de datos sensibles al ser necesario por razones de interés público esencial sobre la base de la normativa educativa, pero deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. De esta forma, sólo podrán acceder a estos datos exclusivamente las personas que requieran esta información para el desarrollo de la función orientadora o docente, además, deberemos implementar medidas específicas de seguridad del tratamiento y evitar el mismo cuando no sea imprescindible.

· Datos biométricos: Se considera como dato de carácter sensible, y son aquellos datos personales relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos y sean obtenidos a partir de un tratamiento técnico específico.

· Datos genéticos: Se considera como dato de carácter sensible, y son aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

PRINCIPIOS DE PROTECCIÓN DE DATOS

Todo empleado del centro que trate datos personales debe seguir unos principios fundamentales:

· Deben ser tratados de manera lícita, leal y transparente.

· Sólo pueden ser recogidos con fines determinados, explícitos y legítimos.

· Los datos deben ser adecuados, pertinentes y limitados en relación con la finalidad del tratamiento.

· Deben ser exactos y, si fuera necesario, proceder a actualizarlos.

· Serán conservados durante no más tiempo del necesario para los fines del tratamiento.

· Es imprescindible que sean tratados garantizando su seguridad.

Los datos han de ser tratados de manera lícita, leal y transparente en relación con su titular. No se pueden recoger ni tratar más datos personales que los estrictamente necesarios para la finalidad perseguida en cada caso, es decir, deben responder a una finalidad legítima, no se pueden recabar de manera fraudulenta y su utilización debe ser conocida por los titulares.

Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Serán exactos y tendrán que estar actualizados, debiéndose suprimir los datos que no son correctos. 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 supresión de los mismos.

La supresión 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.

DERECHOS EN MATERIAL DE PROTECCIÓN DE DATOS

Según el Tribunal Constitucional Español << el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionará a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o no>>.

El Reglamento General de Protección de Datos reconoce el **Derecho a la autodeterminación informativa**, definiéndose como la capacidad del individuo para determinar la divulgación y el uso de sus datos personales, controlar y determinar lo que los demás pueden, en cada momento, saber sobre su vida personal. Este derecho ayuda a los ciudadanos a proteger sus datos personales y, en ejercicio de este

derecho, a autodefinirse y modular su imagen pública y reputación. En definitiva, es la autoridad del individuo para decidir por sí mismo, sobre la base de la idea de autodeterminación, cuándo y dentro de qué límites la información sobre su vida privada debe comunicarse a los demás.

Dentro de las características y elementos que componen el derecho a la autodeterminación informativa destacamos las siguientes:

· Derecho inherente a la persona: Significando que corresponde a todo ser humano por el sólo hecho de serlo, sin necesidad de ninguna otra circunstancia. En virtud de esa inherencia el Tribunal Constitucional considera que afecta a bienes e intereses esenciales y que responde a principios de alcance universal. Por eso, las normas que lo protegen deben ser interpretadas y aplicadas en el sentido más favorable para su efectividad.

· Derecho personalísimo: Esto supone que debe ejercitarlo necesariamente su titular, sin posibilidad de transmitirlo o enajenarlo a otra persona. Es, por tanto, inalienable, indisponible (aunque no se excluye una disponibilidad parcial y concreta en algunos casos, como cuando por vía del consentimiento del interesado se permite la utilización de la propia imagen o se renuncia a la intimidad), irrenunciable e imprescriptible (aunque para algunas acciones concretas sí hay plazo de caducidad).

· Objeto de respeto general: El Derecho a la autodeterminación informativa debe ser objeto de respeto general, pudiendo su titular reclamar protección frente a todos.

· Derecho extrapatrimonial: Debe ser excluido del comercio de los hombres porque carece de valoración económica concreta; así, no puede ser objeto de expropiación, embargo, ni de ejercicio por otro, y no es susceptible de acción subrogatoria. Ahora bien, no atenta contra la extrapatrimonialidad el hecho de que su lesión conlleve una indemnización pecuniaria, forma de reparación normal, aunque no única.

El Derecho a la autodeterminación informativo lo concreta, el Reglamento General de Protección de Datos, en la posibilidad de ejercer ante el responsable del tratamiento los derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.

1) **Derecho de acceso:** derecho que tienen los ciudadanos a que los responsables del tratamiento de datos le informen si están tratando información personal que le concierne y, en caso de respuesta afirmativa, cuáles son esos datos y de qué manera se están tratando. En concreto, el individuo debe poder acceder a la siguiente información:

- Finalidad del tratamiento: los motivos por los que se recaban los datos personales.
- Categorías de los datos personales: datos sensibles, no sensibles y categorías especiales de datos.
- Destinatarios de la información: quiénes son los encargados del tratamiento y quién tiene acceso a los datos.
- Cesión de datos a terceros: si la información va a ser transferida a un destinatario diferente al que la obtuvo.
- Plazo de conservación de datos: el tiempo que permanecerá la información en los ficheros del responsable y/o destinatario, así como los criterios seguidos para determinar dicho plazo.
- Origen de la información: siempre que no se haya obtenido directamente del interesado.
- Existencia de decisiones automatizadas: lo cual incluye informar sobre la elaboración de perfiles y las consecuencias que dichos tratamientos podrían tener para el interesado.

2) **Derecho de rectificación:** supone el derecho a obtener, sin dilación indebida del responsable del tratamiento, la rectificación de los datos personales inexactos que le conciernan o que se completen, según los fines, mediante una declaración adicional. Se deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Además, deberán acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

3) **Derecho de oposición:** derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

4) **Derecho de supresión:** derecho a obtener, sin dilación indebida del responsable del tratamiento, la supresión de los datos personales que le conciernan, cuando concurra alguna de las circunstancias siguientes:
   - Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
   - El interesado retire el consentimiento y este no se base en otro fundamento jurídico.
   - El interesado se oponga al tratamiento.
   - Los datos personales hayan sido tratados ilícitamente.

- Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el derecho de la unión o de los estados miembros que se aplique al responsable del tratamiento.
- Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

5) **Derecho de limitación del tratamiento:** derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:
   - Se impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
   - El tratamiento sea ilícito y las/los interesados se opongan a la supresión de los datos personales y soliciten en su lugar la limitación de su uso.
   - El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
   - Se haya ejercido el derecho de oposición al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

6) **Derecho de portabilidad:** derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
   - El tratamiento esté basado en el consentimiento.
   - El tratamiento se efectúe por medios automatizados.

7) **Derecho de no ser objeto de decisiones individualizadas:** Este derecho pretende garantizar que no seas objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre ti o te afecte significativamente de forma similar.

El derecho a la autodeterminación informativa puede ejercerse en primer lugar ante el colegio que es el que está tratando la información personal de la comunidad educativa. En este caso, se puede solicitar el acceso a dicha información, la rectificación si es incorrecta o la cancelación si se desea que esos datos no sigan tratándose.

Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más. El centro (a través de la dirección) está obligado a informar sobre los medios para ejercitar estos derechos y estos medios deben ser accesibles y no se

puede denegar este derecho por el solo motivo de que se opte por otro medio. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.

Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.

Se pueden ejercer los derechos directamente o por medio de un representante legal o voluntario. Si el colegio tiene dudas sobre la identidad, podrá solicitar información adicional para confirmar la misma como la fotocopia del DNI o pasaporte u otro documento válido que identifique a la persona solicitante. Se puede utilizar la firma electrónica y si se ejercitan a través de un representante se deberá aportar el documento o instrumento electrónico que acredite la representación.

En la solicitud debe incluirse la petición, la dirección a efectos de notificaciones, fecha y firma, así como los documentos acreditativos de la petición si fuesen necesarios.

TRATAMIENTOS DE DATOS POR EL COLEGIO

En el apartado Marco normativo referente a protección de datos (página 3) se hace referencia a la normativa que debe cumplir un centro educativo en cuanto a protección de datos. La mayoría de los tratamientos de datos estarán amparados en la competencia atribuida por una norma con rango de ley, en concreto la Ley Orgánica de Educación, pero en ocasiones realizaremos tratamientos de datos que requerirán el consentimiento informado expreso de las personas interesadas, aunque en el centro se podrá tratar datos sin necesidad de contar con su consentimiento, cuando se trata de datos necesarios para mantener o cumplir la relación laboral o administrativa que mantengan con el colegio.

Cumplir con la Ley de Protección de Datos en el centro educativo es una obligación inevitable, dado el volumen de datos con el que tratamos, desde los del alumnado, maestros/as, personal de servicios y familias, además de tratar datos de menores de edad y de carácter sensible. ¿Cuáles son los datos que tratamos en concreto?

1) Origen y ambiente familiar: Información sobre la situación familiar de los alumnos. El centro puede recoger información relativa tanto a los alumnos como a los padres. El caso de los padres es relevante, ya que si, por ejemplo, están divorciados, el centro debe saber quién ostenta la patria potestad para la recogida de los menores.
2) Condiciones personales del menor: En estos datos pueden aparecer los de carácter sensible (ver página 5) en cuanto sean necesarios para la función

educativa. En este caso hay diferentes momentos en que se pueden recabar datos sensibles del menor, entre los que destacamos:

a. En la matriculación del alumno (Discapacidad, enfermedad crónica, intolerancias alimentarias, alergias…)
b. Durante el curso escolar:
   · Tratamiento médico que reciba un alumno a través del servicio médico o de enfermería.
   · Informes de centros sanitarios a los que se le haya trasladado como consecuencia de accidentes o indisposiciones.
   · Informes de los equipos de orientación psicopedagógica.

3) Desarrollo y resultados de la escolarización del alumno: Se trata de datos e información relacionada con el rendimiento escolar, por ejemplo, las notas de cada uno de los alumnos o como las asignaturas que ellos mismos hayan podido escoger.
4) Circunstancias cuyo conocimiento sea necesario para educar y orientar a los alumnos: Se puede enlazar con los dos primeros apartados, ya que será necesario el conocimiento de la situación familiar y personal del alumno para su buen desarrollo educativo. Por ejemplo, conocer la situación socioeconómica de una familia puede ayudar a determinar si un alumno necesita más o menos apoyo en determinadas áreas o acceso a material escolar.
5) Datos ajustados a la finalidad: No se puede recabar datos personales que sean excesivos para la finalidad para la que son recogidos. Por ejemplo, en el caso de las solicitudes de plaza en un centro de enseñanza, no es necesario recabar los datos bancarios para el pago de actividades extraescolares hasta que no se hubiera resuelto el proceso y fuese admitido el alumno.

Por otro lado, ¿cuáles son los datos con los que nos podemos encontrar y tratar?

1) Lista de admitidos: Se puede publicar la lista de alumnos admitidos en tablones dentro del centro, especial cuidado en la página web del colegio si el acceso no es restringido (como es el caso). Estos datos se pueden publicar siempre y cuando se haga de manera que no suponga un acceso indiscriminado a la información y deberán recoger sólo el resultado final del baremo, no resultados parciales que puedan responder a datos o información sensible o poner de manifiesto la capacidad económica de la familia.
2) Beneficiarios de bonificaciones para los solicitantes de servicios del centro: En estos casos hay que poner en valor dos situaciones.
   a. Si la bonificación está fundada en una situación de discapacidad de los beneficiarios.
   b. Si la bonificación puede afectar a la esfera íntima del afectado.

3) Captación y publicación de imágenes: Si las imágenes obtenidas durante actividades con fines educativos son publicadas en la web del centro deberá contar con el consentimiento de los tutores legales de los alumnos.
4) Publicación de datos personales en la web del colegio: Normalmente en la web del colegio no se publican datos personales, llegado el caso y al ser una web pública, se necesitará consentimiento.

En el colegio vamos a realizar tratamientos de datos legitimados por tres circunstancias diferentes y esto va a suponer que se desplieguen distintos efectos jurídicos:

1) Tratamiento de datos legitimado por una norma con rango legal: El artículo 27.1 de la Constitución Española reconoce el derecho fundamental a la educación y este derecho implica una necesaria actividad administrativa y su consecuente tratamiento de datos personales. El centro puede tratar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa y orientadora, así lo establece la Ley Orgánica de Educación, que habilita el tratamiento de los datos del alumnado con este fin desde el momento en que el alumnado se incorpora al sistema educativo. Igualmente, habilita al colegio, en su caso, para que ceda datos del alumnado en caso de cambio de centro. Asimismo, la Ley Orgánica de Educación habilita a las escuelas para el tratamiento de datos de categorías especiales de datos cuyo conocimiento sea necesario para la educación y la orientación del alumnado. La Ley Orgánica de Educación legitima el tratamiento de datos personales relacionados con el origen y ambiente familiar del alumnado y su familia, características o condiciones personales, datos relativos a la patria potestad y la custodia, datos sobre resultados de la función docente y orientadora, características o condiciones personales del alumnado en cuanto sean necesarios para la función educativa, datos de matriculación del alumnado, discapacidades, enfermedades crónicas, TDAH, intolerancias alimentarias, alergias o tratamientos médicos.
2) Tratamiento de datos por consentimiento expreso e informado. Para todas aquellas otras funciones que no formen parte de la función docente y orientadora del, será necesario contar con consentimiento.
3) Tratamiento de datos legitimado por la relación contractual existente. No se requiere el consentimiento cuando se trata de datos necesarios para mantener o cumplir la relación laboral o administrativa que mantengan con el centro. Se deberán tratar los datos estrictamente necesarios y proporcionales a la finalidad perseguida.

Es importante recordar el principio de proactividad, que exige que el colegio al tratar datos debe informar adecuadamente de estos aspectos, así como, el hecho de que es el centro el que deberá contar con medios probatorios de la existencia de esta

comunicación de la información y de que se ha realizado en los términos que legalmente se establecen.

Como se ha especificado, la normativa educativa legitima al colegio a recabar datos de carácter personal si son necesarios para desempeñar la función docente y orientadora del alumnado. En concreto se pueden recabar:

- Datos identificativos: origen y ambiente familiar y social, características o condiciones personales, datos académicos, financieros o profesionales si el conocimiento es necesario para educar y orientar al alumnado.
- Material audiovisual del alumnado.
- Categorías especiales de datos: por ejemplo, aquellos relativos a la salud del alumnado, cuyo tratamiento se hace para prestar los correspondientes servicios médicos, conocer alergias y/o intolerancias de los alumnos respecto a los servicios de comedor escolar y para adaptar la docencia en función de posibles discapacidades físicas o psíquicas.

Respecto a la información sobre la situación familiar del alumnado que se puede recabar debe estar actualizada y los progenitores han de informar al colegio sobre cualquier modificación. (Es la familia quien debe venir al centro a informar por decisión propia, siendo el centro desconocedor de las situaciones familiares si no lo hacen constar). Debe hacerse hincapié especialmente en los supuestos de modificaciones del régimen de guarda y custodia o de patria potestad para salvaguarda de las personas menores de edad.

Entre los datos relativos a la salud que se pueden recabar en la medida en que sean necesarios para el ejercicio de la función educativa, se pueden distinguir los siguientes momentos:

- En la matriculación del alumnado: 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.

Es muy importante resaltar que 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 están sometidos al deber de guardar secreto como se recoge en el artículo 5 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Los datos recogidos en la matrícula del alumno no se pueden utilizar para finalidades diferentes del ejercicio de la función educativa, como la publicación de fotografías del alumnado en la web del centro o la comunicación de sus datos a museos o empresas para organizar visitas, para ello es necesario recabar el consentimiento de los tutores legales del alumno o de ambos en el caso de familias separadas, después de haberles informado de ello como establece la normativa vigente.

Existen ocasiones en las que el colegio tiene que publicar una serie de datos recogidos en el ejercicio de la función que tiene asignada, por ejemplo relación de alumnado admitido en actividades extraescolares y servicios del centro, relación de beneficiarios de ayudas, menú en el comedor, miembros candidatos al Consejo Escolar, censo para las elecciones del Consejo Escolar… ¿cómo publicar estos datos?.

Cuando se necesite informar sobre las personas que han sido admitidas en la medida en que la admisión se realiza mediante un procedimiento de concurrencia competitiva en el que se valoran y puntúan determinadas circunstancias, la publicidad se realizará de manera que no suponga un acceso indiscriminado a la información, por ejemplo, publicándolo en el tablón de anuncios en el interior del centro. Esta publicación recogerá sólo el resultado final del baremo, no resultados parciales que puedan responder a datos o información sensible o poner de manifiesto la capacidad económica de la familia. Esta información, no obstante, estará disponible para las personas interesadas que ejerciten su derecho a reclamar. Los datos incluidos en los procesos de admisión serán cancelados una vez finalizados los procedimientos administrativos y judiciales de reclamación. Cuando ya no sean necesarios estos listados, hay que retirarlos, sin perjuicio de su conservación por el centro a fin de atender las reclamaciones que pudieran plantearse.

En caso de situaciones de violencia de género la norma específica sobre medidas de protección integral de violencia de género establece que en actuaciones y procedimientos relacionados con la violencia de género se protegerá la intimidad de las víctimas; en especial, sus datos personales, los de sus descendientes y los de cualquier otra persona que esté bajo su guarda o custodia. En consecuencia, el colegio deberá proceder con especial cautela a tratar los datos de los menores que se vean afectados por estas situaciones.

En caso de solicitar bonificación para las actividades extraescolares y servicios del centro, 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, el colegio también podrá

publicar esta información a efectos informativos de los afectados. De forma general, en ningún caso se publicará el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, como mucho, se publicará el nombre, apellidos y 4 cifras de DNI. 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.

El menú del comedor es necesario publicarlo para que las familias estén informadas de la alimentación que sus hijos van a degustar en el colegio, de esta forma, tanto en el tablón del comedor como en la web del colegio será publicado el mismo. Por características culturales, el centro ofrece tres tipos de menú (general, sin carne y sin cerdo), pero sin listado de los alumnos en relación al menú que le corresponde a cada uno de ellos.

Las calificaciones son otros datos que son necesarios publicar, pero en este caso, siempre se hará de forma privada, sin necesidad de que otras personas puedan conocerlas. Se facilitan sólo a los familiares de los alumnos correspondientes mediante mensajería iPasen o de forma presencial en tutorías, de forma que sólo tengan acceso a la información el propio alumno y sus padres y no otras personas distintas a ellas. Aunque, cabe señalar que en la finalización de cada trimestre se realiza un análisis de evaluación con la situación del alumnado en el entorno de su clase, mostrando comparativas frente a la media de los compañeros del aula, sin mostrar en ningún momento relación alguna a nombres concretos.

Los exámenes de los alumnos no se mantendrán más allá de la finalización del periodo de reclamaciones, destruyéndose los mismos seis meses después de su realización. Los datos del expediente académico, en cambio, deben ser conservados, ya que pueden ser solicitados por los alumnos con posterioridad a la finalización de sus estudios.

En ocasiones, el centro puede comunicar datos personales del alumnado a personas distintas de los interesados, por ejemplo peticiones de otros centros educativos (traslados, expedientes…), instituciones y organismos de otras administraciones (Proyectos de Diputación), Servicios Sociales (reuniones de absentismo escolar), de las Fuerzas y Cuerpos de Seguridad (Investigaciones) o de la Administración sanitaria (vacunación, revisión médica, revisión bucodental…). La comunicación de datos requiere, con carácter general, el consentimiento de los interesados, del alumnado o de sus padres o tutores si son menores de 14 años, salvo que esté legitimada por otras circunstancias, como que permita u obligue a ella una Ley, por ejemplo, para solucionar una urgencia médica, o se produzca en el marco de una relación jurídica aceptada libremente por ambas partes, por ejemplo, la establecida

entre los familiares y el centro al matricular a sus hijos o hijas. En estos supuestos se pueden comunicar los datos sin necesidad de obtener el consentimiento de los afectados.

En caso de traslado, la LOE ampara la comunicación de datos al nuevo centro educativo en el que se matricule el alumno o alumna sin necesidad de recabar su consentimiento o el de sus padres o tutores.

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.

A la Administración educativa el colegio comunicará los datos personales del alumnado que sean necesarios para el ejercicio de las competencias que tienen atribuidas las Administraciones educativas como, por ejemplo, la expedición de títulos.

A Servicios Sociales se le aportará información 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.

A las autoridades o sus agentes el centro está obligado a comunicar los datos del alumnado 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 concreto en la reunión de absentismo convocada por el ETMAE (Equipo Técnico Municipal de Absentismo Escolar). En estos casos no ha de mediar solicitud de ninguna autoridad o institución.

Es importante recordar que los datos personales son de los interesados, y que tienen derecho al acceso a los mismos. Por tanto, las personas titulares de los datos podrán acceder a la información relativa al tratamiento de sus propios datos personales.

Los padres, madres o tutores legales, tienen derecho a acceder a los datos, como sujetos que ostentan la patria potestad, entre cuyas obligaciones está la de educar y procurar una formación integral, tienen acceso a la información sobre:

1) Calificaciones y rendimiento escolar
2) Absentismo escolar
3) Cualquier otro aspecto relacionado con la función docente u orientadora.

En los supuestos de patria potestad compartida, con independencia de quién tenga la custodia, ambos progenitores tienen derecho a recibir la misma información sobre las circunstancias que concurran en el proceso educativo del menor, lo que obliga al colegio a garantizar la duplicidad de la información relativa al proceso educativo de sus hijos, salvo que se aporte una resolución judicial que establezca la privación de la patria potestad a alguno de los progenitores o algún tipo de medida penal de prohibición de comunicación con el menor o su familia. En caso de conflicto entre los progenitores sobre el acceso a la información académica de sus hijos, deberá plantearse ante el juez competente en materia de familia.

Tratamiento de datos audiovisuales

En el centro, cada vez más, se va imponiendo el uso de las nuevas tecnologías en el proceso enseñanza-aprendizaje para diferentes tipos de actividades educativas, como las curriculares en las aulas o celebraciones y eventos fuera de ellas, motivo por el que se utilizan herramientas acordes (ordenadores, móviles…) para llevarlas a cabo. El uso de estas herramientas necesitan protocolo y normas de uso para un buen fin, por ejemplo el colegio especifica normas de uso y protocolo para utilizar el móvil en el centro (ver Anexo I).

En las aulas los alumnos utilizan en ocasiones ordenadores portátiles debiéndose comprometer a:

· Comunicar cualquier incidencia al maestro que se encuentre en clase.

· Utilizar el dispositivo únicamente para fines de aprendizaje.

· No conectar el dispositivo a redes abiertas o que no sean de confianza.

· No almacenar datos de carácter personal. En caso de ser necesario, la información deberá estar encriptada.

· No usar la opción “Guardar contraseña” de los navegadores para las credenciales de acceso a aplicaciones corporativas.

· Entregar el equipo a final de curso limpio de contenidos propios.

A principio de curso es obligatorio que los diferentes equipos docentes en reuniones de Ciclo expresen las diferentes aplicaciones que van a utilizar durante el curso, recogiéndose en la programación anual.

En el colegio se trabajan las siguientes aplicaciones:

1) Cuaderno de Séneca para el seguimiento de tareas y evaluación del alumnado.
2) Classroom para la creación y gestión de clases y tareas.
3) Herramientas de OpenOffice para el desarrollo de tareas.
4) Youtube para visionado de vídeos y apoyo a las clases.
5) Actividades interactivas de las editoriales.
6) Genially para generar contenidos digitales interactivos.
7) Quizizz para crear cuestionarios online y trabajar contenidos de forma lúdica.
8) Liveworksheets para digitalizar actividades convirtiéndolas en interactivas.

Si existe la necesidad de utilizar otras aplicaciones a lo largo del curso es necesario solicitar la autorización de uso de la misma a través de la documentación detallada (Anexo II), dirigida al coordinador TDE con registro de entrada, y en cualquier momento del curso escolar, quién después de su evaluación enviará respuesta para su uso.

Para una correcta evaluación de la aplicación educativa a utilizar se debe comprobar si el responsable de la aplicación informa de:

· 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.

Además se debe comprobar que los datos están 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).

El coordinador TDE del centro documentará las evaluaciones realizadas dejando constancia de los aspectos que han sido analizados.

Las aplicaciones que se utilicen deben permitir el control, por parte de familias o profesorado, de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz del alumnado). Al utilizar sistemas de almacenamiento de documentos en nube tipo Dropbox, iCloud o Google Drive, se debe evitar incluir datos personales sensibles, tales como datos relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, etc. En el

marco de la utilización de este tipo de herramientas se recomienda la lectura de la guía de cloud publicada por la Agencia Española de Protección de Datos.

La celebración de eventos escolares (Día de la Paz, Día de Andalucía, Jornadas Escolares de Interculturalidad, Semana del Senderismo…) invita o da paso a tomar fotografías y grabaciones de vídeos, en las que normalmente aparecen imágenes de escolares y maestros. Estos hechos 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:

1) Si la grabación de las imágenes las produce el colegio con fines educativos, como trabajos escolares o evaluaciones, el centro o la Administración educativa estarían legitimados para dicho tratamiento sin necesidad del consentimiento del alumnado o de sus padres, madres o tutores.
2) Si la grabación de las imágenes no se corresponde con una función educativa, sino que se trata de imágenes de acontecimientos o eventos que se graban habitualmente con fines de difusión 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. Para ello se le presentará a cada familia junto a la matrícula una autorización expresa para tal fin (ver Anexo III). Esta autorización se renovará por parte de las familias cada inicio de Ciclos (Infantil 3 años, 1º, 3º, 5º de Primaria y 1º de ESO)

Si existiese el caso de familias en conflicto y alguno de los progenitores no está de acuerdo con la autorización para la grabación de las imágenes de sus hijos o hijas, deberá plantearse ante el juez competente en materia de familia para su resolución; mientras, el centro determina que no podrán publicarse imágenes de sus hijos/hijas hasta la resolución del conflicto.

Importante resaltar que, los padres, las madres y familiares del alumno que decidan tomar fotografías o grabar vídeos en eventos festivos, conmemorativos, deportivos o de otra índole, corresponden a una actividad exclusivamente personal y privada, que se inscriben en el marco de la vida privada, familiar y de amistad, quedando excluidas de la aplicación de la normativa de protección de datos.

En otras ocasiones no es el colegio el que toma las fotografías o vídeos de los alumnos ni tampoco sus familiares, sino que son terceros (monitores de extraescolares, Ayuntamiento, empresa externa…), quien 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. Además,

fuera del colegio, si la grabación se realiza por terceros, por ejemplo, por los responsables de la empresa, museo, exposición o club deportivo que se esté visitando, o en el que se desarrolle una actividad deportiva, será obligación de estos terceros disponer del consentimiento de los interesados que habrán podido recabar a través del centro.

Tratamiento de datos en internet

Entre los datos tratados cabe destacar 3 de especial relevancia:

1) Videovigilancia.
2) Control de horario y seguimiento del personal.
3) Contenido audiovisual de las actividades del centro y servicios educativos.

El centro no dispone de videovigilancia, motivo por el que no desarrollamos este apartado, pendiente si existiese una posible instalación en el futuro. En el caso de instalarse, será preceptivo el cumplimiento de la normativa específica, respetando las limitaciones y obligaciones que se generan en este tratamiento.

Respecto al control de horario y seguimiento del personal del centro se lleva a cabo a través de firma personal en formato papel en el mostrador de conserjería, por supuesto teniendo en cuenta los principios de protección de datos (pág 6). Estas firmas son archivadas en la administración durante el tiempo necesario.

Cuando un maestro tiene que ausentarse del centro por diferentes motivos (personales, médicos, administrativos…) justifica su ausencia con la documentación requerida entregando la misma a la Jefatura de Estudios quien la custodia en una carpeta específica ante posibles requerimientos de inspección. Esta ausencia del empleado es registrada en la aplicación Séneca, adjuntándose el justificante que el empleado entrega al centro y respetando la Jefe de Estudios la privacidad personal.

El colegio hace difusión en internet a través de la página web de actividades culturales, recreativas, deportivas y sociales que lleva a la práctica, como ya se ha indicado en el apartado anterior, es obligatorio para su publicación un consentimiento expreso e informado al encontrarse las publicaciones en un espacio que no exige autentificación e identificación. En la web oficial del centro se publican fotografías de las actividades desarrolladas por el alumnado sin publicar otros datos privados de éstos ni de sus progenitores.

Se descartan diversas redes sociales (Facebook, Telegram, Instagram…) para publicar diferentes eventos llevados a cabo en el centro. Sí se utiliza la aplicación Flickr para adquirir código HTML y con el mismo publicar las fotografías en la web del colegio, de igual modo, el canal de Youtube propio del centro se encuentra oculta pudiéndose visualizar los vídeos sólo en la web oficial del colegio.

La mensajería entre el alumnado y el profesorado se ha realizado a través de la cuenta de google @ceipmigueldecervantes.es, decidiéndose dejar de utilizarla desde el curso escolar 2.023/2.024 y así pasar a utilizar la cuenta @g.educaand.es. En cambio la mensajería entre el profesorado y las familias se realiza a través de iPasen excepto en ocasiones a través de Whatsapp entre la tutoría y la madre/padre delegado.

Tratamiento de datos por la AMPA

La AMPA es una entidad que maneja datos personales tanto de sus miembros como de terceros (por ejemplo un proveedor), por ello tienen la obligación de cumplir con la normativa vigente de protección de datos. En el ejercicio de sus funciones, puede tratar datos de carácter personal tanto de padres o tutores legales como de alumnos, teniendo poder de decisión sobre la finalidad, el uso y el contenido de dichos datos, siendo, por tanto, responsables de su tratamiento. Son datos de carácter personal identificativos de padres o tutores legales y alumnos, además, también pueden tratar datos personales de carácter económico, profesionales o sociales, incluidas también imágenes de las actividades que se puedan llevar a cabo en el centro y permitan identificar a las personas que aparecen en ellas. Pero los datos personales donde más cuidado debe poner esta asociación respecto al cumplimiento normativo, es respecto a aquellos correspondientes a los menores de edad, puesto que se les considera un colectivo vulnerable.

Respecto a los datos personales de los alumnos del centro, el AMPA sólo podrá llevar a cabo un tratamiento cuando:

1) Gestionen un servicio escolar (comedor, transporte…), en cuyo caso, el responsable del tratamiento seguirá siendo el centro y la AMPA ejercerá como encargado del tratamiento, además, sería necesario firmar un contrato entre el centro y asociación que contenga todas las garantías necesarias.
2) Organicen actividades extraescolares o similares.

Los datos que gestione el AMPA deben ser tratados siempre con el máximo rigor y garantías y atendiendo al principio de mínima conservación de los datos, por lo que se recogerán y se tratarán los datos estrictamente necesarios (calidad de los datos). Resulta imprescindible tener en cuenta tres aspectos fundamentales:

1) La forma en la que se recogen los datos. Se debe garantizar su confidencialidad y veracidad. Además de contar con el debido consentimiento.
2) El destino que se da a los datos recogidos. Estrictamente debe circunscribirse a las funciones y obligaciones del AMPA.

3) El principio de información. Los titulares deben de estar informados por el responsable de todos los aspectos relativos al tratamiento de los datos.

La AMPA puede publicar en ciertos casos datos personales de alumnos y/o familiares cuando para ello cuenten con el consentimiento expreso de los mismos, previa información sobre la finalidad de la publicación. Estas publicaciones se realizan, normalmente, en sus redes sociales, y los datos que se publican son los nombres de los alumnos e imágenes y vídeos de actividades escolares o extraescolares en los que puedan aparecer y ser reconocibles alumnos y/o sus familiares. En el caso de los alumnos, además, la edad mínima para poder dar su consentimiento para estas publicaciones es de 14 años, por debajo de esa edad, son ambos progenitores o el tutor legal del menor, los que deben dar el consentimiento.

Las obligaciones y requisitos que establece el RGPD para la AMPA tiene un doble carácter, por un lado tiene obligaciones documentales y, por otro lado, operativas y de funcionamiento. Las obligaciones documentales son aquellas relacionadas con la elaboración de documentos e informes necesarios para documentar la correcta aplicación de la normativa de protección de datos, como pueden ser el registro de actividades de tratamiento o el análisis de riesgos. Mientras que las obligaciones operativas y de funcionamiento son aquellas medidas que debe aplicar la AMPA para adecuar su funcionamiento a las exigencias del RGPD.

INFORMACIÓN Y FORMACIÓN

Informar y formar a la comunidad educativa en materia de protección de datos es una obligación que el colegio debe cumplir. Además, siguiendo con el principio de responsabilidad proactiva se deberá implementar un plan de información y formación que permita y promueva el respeto y el cumplimiento de la normativa vigente por parte de las personas encargadas del tratamiento de datos en el desarrollo de sus funciones en la organización.

Se hace necesario difundir una cultura de protección de datos entre las personas encargadas del tratamiento con el objetivo de sensibilizar a quienes los manejan y sean responsables del mismo, así como conocer las normas de seguridad que afecten al desarrollo de sus funciones y las consecuencias en que pudiera incurrir en caso de incumplimiento.

El centro deberá:

- Informar a la comunidad educativa en los términos establecidos legalmente, cuando se realice tratamientos de datos en cumplimiento de una obligación establecida por imperativo legal.

- Informar a la comunidad educativa del uso de las aplicaciones y almacenamiento en la nube utilizado en el ejercicio de las funciones atribuidas legalmente, después de haberlas evaluado e incorporado en el Plan de Centro.
- Impulsar programas informativos. Se debe establecer programas de concienciación orientados hacia la protección de los datos personales, dirigidos a profesorado y alumnado, sobre la importancia del uso correcto de aplicaciones.
- Ofrecer y facilitar formación de protección de datos a todo el profesorado y al personal de servicios que vaya a realizar actividades de tratamiento de datos.
- Formación básica relacionada con seguridad y ciberseguridad para el tratamiento de datos.

Al inicio de cada curso escolar en reunión de Claustro se dará a conocer la existencia del presente Protocolo, para que en reuniones de Ciclo previstas en los días de organización del curso (del 1 al 10 de septiembre) los diferentes miembros de cada Ciclo puedan analizarlo y comprenderlo. Es importante su análisis pues son ellos quienes posteriormente lo darán a conocer a las familias que acudan a la reunión de tutoría inicial, informándoles a su vez que el presente Protocolo lo tendrán disponible en la web del centro.

Cada curso escolar el colegio participa en el Programa “Plan Director”, contando con el apoyo de las Fuerzas y Cuerpo de Seguridad del Estado para explicarles al alumnado los riegos de internet, fraudes, protección de datos…, jornadas muy interesantes para su formación. Además, este mismo servicio se le ofrece a la AMPA para que también pueda informarse y formarse.

POLÍTICAS DE SEGURIDAD Y CIBERSEGURIDAD

De todas las normas aplicables a la seguridad y ciberseguridad debemos destacar el Reglamento Europeo de Protección de Datos y la normativa española de desarrollo: la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, que velan por la protección y privacidad de los datos personales. En ellas, se señala la obligación de crear una política de seguridad en los centros educativos, así como la necesidad de informar y formar a la comunidad educativa de la misma.

Todas las normas relacionadas con las medidas de ciberseguridad responden a la Estrategia Nacional de Ciberseguridad, que delimita el entorno del ciberespacio y fija los principios, objetivos y líneas de acción que garantizan la ciberseguridad nacional.

En el ámbito de ciberseguridad existen una serie de conceptos importantes a tener en cuenta:

· Ciberseguridad: Conjunto de estrategias que a través de herramientas, políticas y procesos procuran la protección de la infraestructura computacional y la información contenida en un dispositivo o que circula por redes.

· Autenticación: Es el proceso que permite la verificación de la identidad de una persona cuando intenta acceder a archivos o un dispositivo.

· Copia de seguridad: Almacenamiento de copias de sus archivos en un servidor, disco duro, ordenador o unidad extraíble para acceder a ellos en caso de pérdida.

· Red Privada Virtual (VPN): Estrategia que persigue ofrecer un sistema más seguro de acceso a Internet mediante el enrutamiento de la conexión a través de un servidor que oculta su ubicación.

· Cifrado: Procedimiento que permite la transformación de datos para ocultarlos.

· Firewall: Hardware o software diseñado para mantener a los usuarios no deseados fuera de su red.

· Evaluación de riesgos: Proceso de identificación de posibles riesgos a los que se enfrenta una institución y la red.

· Robo de datos: Se define como el acceso no autorizado a datos.

· Hacker: Persona que infringe la seguridad para acceder a los datos con una intención maliciosa.

· Malware: Software diseñado para llevar a cabo acciones perjudiciales y no autorizadas en un ordenador.

· Phishing: Estafas por correo electrónico enviadas por hackers para obtener información confidencial como información bancaria o contraseñas.

· Spyware: Software espía malicioso que roba datos personales sin consentimiento.

· Virus: Malware diseñado para propagarse automáticamente.

· Gusano: Malware que se instala en un ordenador y se copia a sí mismo en otros equipos.

Poder trabajar con internet en el colegio nos ofrece muchas posibilidades de información y formación, pero también nos supone tener que asumir una serie de riesgos. Éstos, según Pere Marqués, se pueden clasificar en:

1) Riesgos relacionados con la información:
   · Acceso a información poco fiable y falsa.
   · Dispersión, pérdida de tiempo.
   · Acceso de los niños a información inapropiada y nociva para su edad.
   · Acceso a información peligrosa, inmoral, ilícita (pornografía infantil, violencia, racismo, terrorismo,)
2) Riesgos relacionados con la comunicación:
   · Bloqueo del buzón de correo.
   · Recepción de “mensajes basura”.
   · Recepción de mensajes ofensivos.

· Pérdida de intimidad.
· Acciones ilegales: difundir datos de terceras personas, plagiar, amenazar…
· Malas companies.

3) Riesgos relacionados con las actividades económicas:
· Estafas.
· Compras inducidas por publicidad abusiva.
· Compras por menores sin autorización paterna.
· Robos.
· Actuaciones delictivas por violación de la propiedad intelectual.
· Realización de negocios ilegales.
· Gastos telefónicos desorbitados.

4) Riesgos relacionados con las adicciones:
· Adicción a buscar información.
· Adicción a frecuentar las Redes Sociales.
· Juego compulsivo.
· Compras compulsivas.

Si se materializan estos riesgos podríamos estar ante las siguientes situaciones:

· Ciberbullying. Se trata del acoso de un menor a otro menor usando las tecnologías: Internet, móvil, videojuegos online, etc. Estamos ante un caso de ciberbullying cuando una persona menor de edad atormenta, amenaza, hostiga, humilla o molesta a otros menores usando estos medios.

· Ciberacoso o acoso cibernético. Se trata de una situación en la que una persona utiliza un perfil en internet, normalmente falso, para amenazar y acosar anónimamente a una persona en específico. Las víctimas de acoso cibernético tienen que enfrentar problemas psicológicos que interfieren con su vida diaria (trabajo, escuela, etc.).

· Grooming**.** Estamos ante grooming cuando una persona adulta trata de engañar a un menor a través de Internet para ganarse su confianza con intención de obtener fotos o vídeos de situaciones sexuales o pornográficas e incluso llegar a chantajearle con ellas. En ocasiones es el paso previo al abuso sexual.

· Sexting**.** Consiste en enviar mensajes, fotos o vídeos de contenido erótico y sexual personal a través del móvil mediante aplicaciones de mensajería instantánea o redes sociales, correos electrónicos u otro tipo de herramienta de comunicación.

· Phishing**.** Se trata de un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar

· Suplantación de identidad**.** Se trata de una actividad malintencionada que consiste en hacerse pasar por otra persona por diversos motivos: cometer algún tipo de fraude, obtener datos de manera ilegal, cometer ciberacoso, grooming u otros delitos.

· Ciberadicción o trastorno de adicción a internet, término que se refiere a una supuesta patología que supone un uso abusivo de Internet, a través de diversos dispositivos (ordenadores, teléfonos, tabletas, etc.), que interfiere con la vida diaria.

Ya en el apartado Tratamiento de datos audiovisuales (página 17) se especifica a qué debe comprometerse el alumnado para el buen uso de móviles y ordenadores en el colegio. De todas formas, además, se debe tener en cuenta los siguientes aspectos para una correcta política de seguridad:

1) Avisar al maestro cuando detectemos errores o extraño comportamiento de los equipos informáticos. Posteriormente el maestro al que se ha avisado se lo comunicará al coordinador TDE.
2) Disponer con un firewall confiable y actualizado para ayudar a identificar amenazas y conductas sospechosas.
3) Disponer de un buen antivirus actualizado y cortafuegos.
4) Realizar copias de seguridad a menudo para no perder información ante posibles incidencias.
5) Habilitar las actualizaciones automáticas para el sistema operativo.
6) Verificar los remitentes de los emails que se reciben. No abrir los que inspiren desconfianza o duda.
7) Antes de descargar archivos o entrar en páginas indicadas en un email, se debe comprobar su origen.
8) Desconfiar de ventajas exageradas, películas gratis, promociones de gran beneficio… nos pueden guiar a descargar malwares mal intencionados.
9) Actuar con calma y sentido común ante mensajes que implican urgencia para realizar alguna acción.

Es imprescindible que la comunidad educativa conozca y se comprometa con la política de seguridad del colegio. Para ello, deberán adquirir una competencia digital básica en esta área que les permitan realizar un uso responsable de las herramientas de seguridad implementadas, así como incorporar buenas prácticas en su proceder habitual. En la web oficial del INCIBE se publican itinerarios formativos especializados en diferentes sectores, entre ellos el sector educativo. Los itinerarios consisten en cortos videos interactivos presentados por dos personajes ficticios: Laura y Miguel, que representan a dos socios preocupados por la ciberseguridad de su organización. Ellos mostrarán las distintas situaciones cotidianas que pueden afectar a las diferentes instituciones y las acciones que debemos implementar para protegerlas.

Ver vídeos de itinerarios

Existen una serie de recomendaciones básicas que se deben cumplir en cumplimiento del código de conducta legalmente vigente, algunas ya comentadas:

1) Los maestros/as que hagan uso de equipamientos TIC no podrán modificar el software que se encuentre instalado en los mismos.
2) Se deberán mantener actualizados tanto los antivirus como los sistemas operativos.
3) No se deberán instalar programas no autorizados.
4) Se deberán realizar copias de seguridad habitualmente.
5) Sólo abriremos correos de remitentes conocidos.
6) Sólo trabajaremos en entornos seguros.
7) Es imprescindible asegurar los dispositivos con contraseñas, PIN o información biométrica.
8) Es recomendable encriptar y asegurar la información sensible.
9) Antes de instalar aplicaciones debemos revisar los permisos y eliminar las aplicaciones que no usemos, desinstalándolas.
10) Deberemos utilizar contraseñas largas y alfanuméricas y diferentes para las distintas cuentas y redes sociales.

Respecto a las contraseñas deben ser seguras, pero… ¿qué se considera una contraseña segura? Según la "Guía de Seguridad de las TIC CCN-STIC 821. APÉNDICE V: NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS NP40":

· Las contraseñas deberán tener una longitud mínima de 8 caracteres y ser alfanuméricas.

· Se recomienda la utilización de la concatenación de varias palabras para construir contraseñas largas cuya deducción, automática o no, no sea simple.

· Las contraseñas no deben estar compuestas de datos propios o de otra persona que puedan ser adivinadas u obtenidas fácilmente como el uso de nombre, apellidos, fecha de nacimiento, etc, ni ser frases famosas o refranes, ni estrofas de canciones.

· No es recomendable apuntarlas en papel o en otro procedimiento o contenedor no seguro, las contraseñas deben tener carácter secreto, no debemos comunicarla a nadie.

· Es imprescindible cambiarlas con una cierta periodicidad (Por ejemplo 1 año). Del mismo modo las sustituiremos antes si existe evidencia de que hubieran sido comprometidas.

· No deberemos utilizar la misma contraseña para distintos servicios web o el acceso a distintos dispositivos.

Cada día se utilizan más los teléfonos móviles y tablets tanto para el trabajo del docente como el desarrollo de actividades de los discentes, por ello también es importante tener en cuenta una serie de medidas:

· Bloquear el acceso con contraseña.

· Cifrado de datos introduciendo código secreto para visualizar información.

· Bloqueo del terminal y la tarjeta SIM ante situación de robo o extravío.

· Copia de seguridad en otro equipo.

· Antivirus y softwareactualizado.
· Utilizar redes wifi seguras.

Para el correo electrónico se debe tener en cuenta las siguientes medidas para un uso correcto y seguro:
· Utilizar el correo corporativo en el ámbito del colegio.
· Cifrado de los correos electrónicos.
· Realizar una gestión adecuada del correo sospechoso o no deseado.
· Crear una política corporativa de correo electrónico.
· Guardar de forma segura la contraseña del correo.
· Realizar copias de seguridad de correos y contactos.

ANEXO I

NORMAS Y PROTOCOLO DE USO DE DISPOSITIVOS MÓVILES PARA EL APRENDIZAJE (documento para la familia)

El CEIP Miguel de Cervantes informa a su comunidad educativa de que el uso de los teléfonos móviles están **prohibidos** en el centro, salvo para actividades curriculares requeridas. Con este documento pretendemos establecer un protocolo y normas de uso sobre la utilización de dispositivos móviles con la finalidad de regular y lograr su correcta integración en las aulas, en la vida escolar y en definitiva en el proceso educativo, tanto humano como académico, del alumno/a.

Estas normas y protocolo, se deben entender como un anexo del Reglamento de Organización y Funcionamiento interno del centro, el cual tiene por función primordial promover y ordenar la vida diaria del Centro Educativo, así como la adopción de normas reguladas o no por ley, que permitan el buen funcionamiento del Colegio y la convivencia entre los distintos miembros de la comunidad educativa.

Por todo ello, se ha considerado adecuado establecer el siguiente protocolo para el uso de los distintos dispositivos móviles para el aprendizaje que puedan utilizarse en el centro:

1. El dispositivo móvil, es una herramienta de trabajo y estudio.

2. El alumnado depositará el móvil cada día en la bandeja específica de su clase, custodiándose la misma en la dirección del centro, pudiéndose recoger la bandeja o los móviles por el alumno/a asignado por el maestro/a.

3. Únicamente puede utilizarse en el aula y fuera de ella para la realización de aquellas tareas o usos que haya solicitado y autorizado un/a profesor/a, siempre bajo su supervisión.

4. Durante el horario escolar los dispositivos son de uso exclusivamente académico y, por tanto, no se puede escuchar música, ver o hacer fotos, entrar en portales no educativos, chatear, hacer descargas, utilizar redes sociales, etc.

5. La Ley de Autoridad del Profesor reconoce la condición de autoridad pública de los directores y demás miembros del equipo directivo, así como del resto de profesores de los centros educativos públicos. Esta condición de autoridad pública les habilita para que puedan adoptar medidas provisionales cuando pudieran cometerse conductas contrarias a las normas de convivencia del centro, con el fin de garantizar el normal desarrollo de las actividades educativas. En todo caso, la adopción de estas medidas será comunicada a los padres o tutores legales del alumno/a.

6. El/la profesor/a que se encuentre en el aula, en el ejercicio de sus funciones, podrá supervisar, comprobar y corregir las actividades que se estén llevando a cabo y el

contenido de éstas, asegurando además que el uso está siendo el adecuado y que están abiertas sólo las aplicaciones que se precisan para esa clase o actividad educativa.

7. Aprender con dispositivos móviles no excluirá del uso de otros soportes, herramientas y materiales escolares que puedan necesitarse.

8. A tenor del Reglamento General de Protección de Datos 2016/679, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, queda prohibido grabar imágenes o audio dentro del centro. La utilización de imágenes de profesores y compañeros sin la debida autorización es un delito tipificado y penado por la ley.

9. Los daños a terceros se penalizarán con la reposición del material dañado por parte del responsable.

10. Se recomienda a las familias participar en las orientaciones, consideraciones, sesiones, cursos y pautas que proporcione el centro que sirvan de ayuda en su formación para el uso seguro, adecuado y correcto de dispositivos móviles, redes sociales, Internet, etc.

11. Si algún alumno/a incumpliera alguna de estas normas y protocolo de uso de dispositivos móviles en el aula y en el centro, se procederá a amonestación verbal y a la limitación temporal del uso del dispositivo en el centro si fuese necesario. El teléfono será retirado por la dirección del centro y guardado hasta que la familia venga a recogerlo. Si estas acciones son reiteradas, será la Comisión de Convivencia del Consejo Escolar la que establezca la sanción adecuada.

12. El centro no se hace responsable del mal uso que pudiera llevarse a cabo del dispositivo fuera del horario escolar.

13. El uso de los dispositivos móviles es exclusivo para el alumnado de 1º y 2º de ESO. Queda terminantemente prohibido el uso para el alumnado de E. Primaria y por tanto, no podrán traer el teléfono al centro.

MODELO DOCUMENTO DE CONSENTIMIENTO INFORMADO Y AUTORIZACIÓN DE CONTROL DEL DISPOSITIVO MOVIL

1.- Recibimos y entendemos las NORMAS Y PROTOCOLO DE USO DE DISPOSITIVOS MÓVILES PARA EL APRENDIZAJE y nos comprometemos a cumplir con los términos señalados en el mismo.

2.- Conocemos la responsabilidad de nuestro/a hijo/a y, por la tanto, la nuestra propia, a la hora de utilizar la red inalámbrica del Centro (la wifi) en nuestro dispositivo móvil y entendemos que el acceso a la red de Internet del Centro es solo con fines educativos.

3.- Entendemos y aceptamos que el mal uso de los equipos tecnológicos o de la red inalámbrica puede conllevar sanciones tipificadas como faltas leves, graves o muy graves, recogidas en el propio Plan de Convivencia del Centro, sin perjuicio de otras responsabilidades civiles o penales que pudiera causar el mal uso del dispositivo, tanto al centro como a terceros.

Nombre y Apellidos del alumno/a: _____

Curso: _____

Nombre y Apellidos de padre/madre/tutor legal: _____

DNI: _____

Marca con una X si NO autorizas o SI autorizas

☐ SÍ autorizamos este control del dispositivo en el horario escolar.

☐ NO autorizamos este control del dispositivo en el horario escolar.

Lucena del Puerto, a ____ de _____ de 20___

Fdo: _____

ANEXO II

SOLICITUD DE AUTORIZACIÓN DE USO DE APLICACIÓN DIGITAL

D/Dª _____ , como maestro/a titular de la area _____ del grupo_____ de Primaria/Secundaria durante el curso escolar _____ .

Expone:

Hacer uso de la aplicación educativa _____ como herramienta para desarrollar contenidos del área que imparto en el grupo indicado durante el tiempo que imparta clases.

Solicito:

Evaluación y autorización de la aplicación educativa mencionada durante las clases que imparto en el grupo indicado.

Lucena del Puerto, a ___ de _____ del 20___

Fdo: _____

D.N.I. _____

(El maestro/a que pide el manejo de la aplicación solicitada se hace cargo de las incidencias ocasionadas por su uso)

ANEXO III

Autorización para la publicación de imágenes/contenido audiovisual del alumnado

En cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos 2016/679 de 27 de abril de 2016, se le informa que las fotografías, vídeos y demás contenido audiovisual en las cuales aparezca su imagen individualmente o en grupo realizadas durante las actividades culturales, recreativas, deportivas y sociales en las que participa el centro educativo en sus instalaciones y/o fuera de las mismas serán incorporados para su tratamiento al fichero 'Contenido audiovisual de las actividades de los centros y servicios educativos' con la finalidad educativa no comercial de difundir, visibilizar, compartir buenas prácticas y promocionar las citadas actividades.

El interesado autoriza a la Dirección del C.E.I.P. “Miguel de Cervantes” (Código 21002288) a ceder a partir de este momento sus datos personales en las publicaciones del propio centro, para su utilización en las finalidades arriba expuestas referidas a la programación educativa de los cursos _____ y _____

El responsable del tratamiento es la Consejería de Educación de la Junta de Andalucía y la dirección del C.E.I.P. “Miguel de Cervantes” (Código 21002288)

Si lo desea, podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos en el C.E.I.P. “Miguel de Cervantes” (Código 21002288), sito en Plaza de Andalucía s/n, 21820 Lucena del Puerto (Huelva) o a través del correo electrónico 21002288.edu@juntadeandalucia.es. Sin perjuicio de otras acciones que le reconoce la legislación actual.

Igualmente se le recuerda que podrá retirar su consentimiento en cualquier momento sin alegar causa manifestando su intención a través del correo electrónico 21002288.edu@juntadeandalucia.es.

En consecuencia, la Dirección del C.E.I.P. “Miguel de Cervantes” (Código 21002288) solicita su consentimiento informado: (marque con una cruz lo que proceda)

☐ Doy mi CONSENTIMIENTO ☐ NO doy mi CONSENTIMIENTO

En caso de ser un alumno o alumna menor de catorce años, la madre, padre o tutor legal debe acreditar el consentimiento informando los datos que a continuación se indican:

Don/Doña _____ con DNI _____

como padre/madre o tutor de _____

con domicilio a efectos de notificaciones en _____