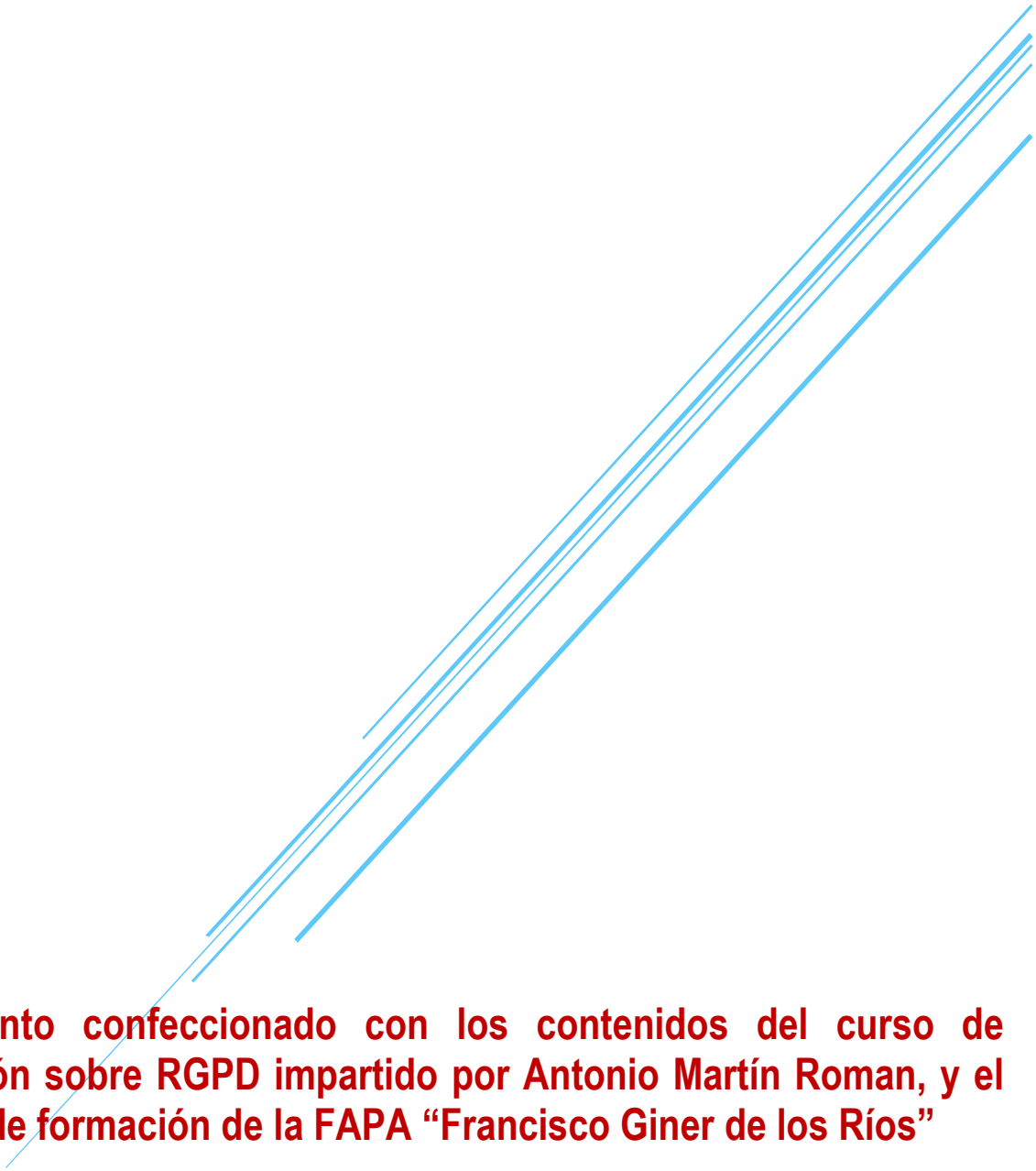
DOCUMENTACIÓN SOBRE PROTECCIÓN DE DATOS



Documento confeccionado con los contenidos del curso de formación sobre RGPD impartido por Antonio Martín Roman, y el equipo de formación de la FAPA "Francisco Giner de los Ríos"

MANUAL DE PROTECCIÓN DE DATOS

INTRODUCCIÓN

En este documento queremos recoger de forma sintetizada las cuestiones más relevantes sobre el nuevo Reglamento de la UE 2016/679 del Parlamento Europeo y el 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, esta norma deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Este Reglamento sustituye la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (normativa española), mientras se desarrolla una nueva Ley Orgánica, que se adapte al nuevo Reglamento, pero hasta que se apruebe el nuevo RGPD es de obligado cumplimiento.

¿CÓMO NOS AFECTA?

Las asociaciones de madres y padres de alumnado somos entidades con identidad jurídica propia, que tienen que tomar decisiones sobre la finalidad, uso y contenido de los datos personales que se solicitan a los asociados, por lo tanto, somos responsables de su tratamiento y de la protección de esa información y debemos cumplir con las obligaciones de la normativa sobre protección de datos.

Para ejercer sus funciones pueden tener que tratar datos de carácter personal del alumnado, madres, padres, tutoras, tutores, cargos de la asociación, personas que prestan servicios al AMPA o, en general, de terceras personas con las cuales se relacionan.

Las AMPAS pueden tener que tratar datos identificativos, de características personales, académicas y socio económicas entre otros y en algunos casos también datos especialmente protegidos.

CONCEPTOS BÁSICOS QUE DEBEMOS CONOCER

El afectado o Interesado. Persona física titular de los datos que sean objeto de tratamiento (alumnado, empleados, padres, madres, tutores, tutoras, proveedores, etc.).

Responsable del fichero o tratamiento. Es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso de este mismo, bien por decisión directa o porque así le viene impuesto por una norma legal. **En nuestro caso la AMPA**.

Responsable de seguridad. Persona o personas a las que el responsable del fichero ha asignado, formalmente, la función de coordinar y controlar las medidas de seguridad aplicables. *Suele recaer en la presidencia de la asociación o en un cargo orgánico.*

Encargado del tratamiento. Es la persona (física o jurídica, pública o privada, u órgano administrativo) que, solo o conjuntamente a otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. *Son los encargados de manejar esos datos personales, puede ser una o varias personas de la asociación o de una empresa que se tenga contratada para ese cometido.*

Delegado de Protección de Datos. Deberá contar con conocimientos especializados del Derecho, y obviamente en protección de datos, que actuará de forma independiente. Se le atribuirán una serie de funciones reguladas en el artículo 39 del RGPD, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado. NO AFECTA A LAS AMPAS PORQUE LOS DATOS QUE SE MANEJAN NO SON ESPECIALMENTE PROTEGIDOS.

Hay que poner especial empeño en:

- El cumplimiento del deber de información del interesado y en su caso, la obtención del consentimiento para el tratamiento de su información de carácter personal ***(Anexo 1)*.**
- Formalización de contratos de acceso a datos por cuenta de terceros y contratos de prestación de servicios sin acceso a datos por terceros ***(Anexo 8-Modelo de Documento de Seguridad)*.**
- Elaboración del Documento de Seguridad e implantación de medidas de seguridad de carácter técnico y organizativo en el sistema de información ***(Anexo 8- Modelo de Documento de Seguridad)*.**
- Formación del personal, usuarios y responsables de seguridad ***(Anexo 8-Modelo de Documento de Seguridad)*.**

Si no se cumple la normativa las sanciones económicas pueden ser, o bien de diez millones de euros o el equivalente al 2 % de la facturación anual total de una corporación, o bien de veinte millones de euros o el equivalente al 4 % de la facturación anual de la empresa.

Con esta nueva normativa ya no es obligatorio que el responsable del fichero (AMPA), notifique e inscriba los ficheros creados para el tratamiento de datos ante el Registro de Protección de Datos, así como comunicar las modificaciones o cancelaciones con respecto a los mismos; inscripción a la que nos obligaba la Ley Orgánica 15/1999, de 13 de diciembre.

Sobre qué debemos informar (*en la ficha de recogida de los datos*):

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos *(**si no se da los datos, no se puede ser socio**)*.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del Responsable del Tratamiento.

¿QUÉ ES ARCO Y DERECHO DE PORTABILIDAD?

ARCO es el acrónimo de las palabras acceso, rectificación, cancelación y oposición, cuestiones que hay que facilitar a las personas de quien tenemos datos.

- ACCESO. El afectado o interesado, tiene derecho a conocer ***(Anexo 2)***:
  - Qué datos tenemos de él.
  - El origen de sus datos *(cómo los hemos recabado)*.
  - Comunicaciones realizadas o que se pretendan realizar, identificando a los cesionarios *(la cesión que hayamos hecho o vayamos a hacer de los datos, para el desarrollo de las actividades: empresa de comedor, desayunos, servicio de canguro o empresa de extraescolares)*.
  - Usos concretos y finalidades para las que necesitamos tener sus datos *(gestionar las actividades extraescolares, informar de las asambleas, reuniones o convocatorias de la AMPA…)*.

La AMPA deberá atender la solicitud en un plazo máximo de 1 mes desde la recepción de la solicitud. En caso de estimarse procedente, permitir el acceso en 10 días hábiles. El responsable del fichero está obligado a responder incluso cuando no trate datos personales de quien ejercite el derecho *(p.* e., para comunicarle que no disponemos de sus datos personales, si es este el caso).

- RECTIFICACIÓN. Cuando los datos sean inexactos, incompletos, inadecuados o excesivos. La AMPA dispone de un máximo de 10 días hábiles desde la recepción de la solicitud ***(Anexo 3)***.

- CANCELACIÓN. Cuando exista la voluntad por parte del interesado, de que no se traten sus datos. El AMPA deberá comunicar al cesionario, en el plazo de 10 días hábiles, la cancelación llevada a cabo ***(Anexo 4)*.**

Excepciones:

- Cuando exista una obligación de conservar los datos *(se tiene que conservar los datos de los socios, mientras se es socio, se deben de mantener los datos de éste)*.
- Cuando la cancelación no sea posible por razones técnicas.

- OPOSICIÓN. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique siempre que una Ley no disponga lo contrario. El AMPA dispone de un plazo de 10 días hábiles desde la recepción de la solicitud ***(Anexo 5)*.**

Derecho de portabilidad. El interesado podrá requerir al AMPA que sus datos personales sean facilitados a otra empresa o asociación facilitados en un formato estructurado, de uso común y lectura mecánica, y poder transmitirlos a otro responsable, siempre que sea técnicamente posible.

¿QUÉ ES UN DATO DE CARÁCTER PERSONAL?

Dentro del artículo 4 del Reglamento se recogen diferentes definiciones y define datos de carácter personal como*: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular a través de un identificador (un nombre, un número, datos de localización, elementos propios de la identidad física, genética, psíquica, económica, cultural, etc.).*

El nombre y apellidos del alumnado, de sus padres, madres, tutores y tutoras, su dirección, su número de teléfono o su correo electrónico son datos de carácter personal. También lo son las imágenes de los alumnos y alumnas o, por ejemplo, la profesión, los estudios o el lugar donde trabajan los padres, madres, tutores y tutoras, o su número de cuenta bancaria. No se pueden recoger ni tratar más datos personales que los estrictamente necesarios para la finalidad perseguida en cada caso y su utilización debe ser conocida por los titulares. Si se recogieron datos para realizar una actividad en concreto, no se podrán utilizar para finalidades diferentes salvo que se haya recabado el consentimiento del alumnado o, en caso de los menores de 14 años, de sus padres, madres, tutores o tutoras, tras haberles informado de ello.

Hay que tener cuidado con los datos especialmente protegidos y estos son:

- Los que revelen ideología, afiliación sindical, religión y creencias.
- Hagan referencia al origen racial, a la salud *(alergias, TDAH, discapacidades físicas o psíquicas, celiaquía, diabetes u otras enfermedades, que debieran conocer los monitores de actividades extraescolares o del desayuno, comedor, campamentos…)* y a la vida sexual.
- Se refieran a la comisión de infracciones penales o administrativas *(el certificado de delitos sexuales, si es positivo, no puede trabajar de monitor; si es negativo, no es dato especialmente protegido)*.

A efectos del reglamento se podrá utilizar la seudonimización. Que es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable *(p. e., asignando a cada dato médico una clave, sólo conocida por la persona que la graba y la persona que la tiene que utilizar. Guardar en las fichas los datos médicos con esas claves, sin nada que permita descifrarla).*

ACTUACIONES CON LAS EMPRESAS DE PRESTACIÓN DE SERVICIOS

Las empresas contratadas para actividades, comedor… Las empresas *(terceros)* que sean contratadas por la AMPA para prestar los servicios de actividades extraescolares, transporte escolar, comedor, etc., tienen la consideración de encargados del tratamiento de datos personales *(ver descripción en apartado de datos de carácter personal)*.

Prestación de servicios por terceros con acceso a datos. La prestación de servicios por terceras personas o entidades que comporta el acceso a datos personales de los ficheros o de los sistemas de que es responsable la AMPA, requiere la suscripción del contrato o el acuerdo de encargo y se considera un encargado de tratamiento *(Anexo INFo05, del Anexo 8-Modelo de Documento de Seguridad), se relacionarán los terceros que actúan como encargados del tratamiento por cuenta de la AMPA, con indicación de si los datos necesarios para prestar los servicios se tratan en los locales de la AMPA o bien en los del encargado de los ficheros o tratamientos afectados por el encargo, y del contrato o acuerdo de encargo suscrito y su vigencia)*.

El encargado del tratamiento tiene que guardar secreto y confidencialidad sobre los datos personales de los ficheros a los cuales tiene acceso para prestar el servicio encargado.

CESIÓN DE DATOS

Cuando se comunican los datos del alumnado de un centro a asociaciones de madres y padres, (AMPA), a los Servicios Sociales o Sanitarios, Jueces, Tribunales, Cuerpos y Fuerzas de Seguridad se produce una cesión de datos.

No son cesiones de datos, las comunicaciones de los datos del alumnado a las empresas para que, en nombre, y previo contrato con el AMPA, presten servicios (p. e., de comedor, médico o transporte).

MEDIDAS DE SEGURIDAD

Medidas que se deben de adoptar para la custodia de los datos personales.

- Establecer medidas de carácter técnico y organizativo que garanticen la seguridad de los citados datos (su integridad, confidencialidad y la protección) frente al tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.
- En la actualidad, el desarrollo del RGPD, determina las medidas de seguridad en tres niveles, básico, medio y alto. Las AMPAS, normalmente, trabajarán con los datos de nivel básico.
- Todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre los mismos. Es de obligado cumplimiento **incluso una vez finalizada la relación.**

Hasta cuándo se conservarán los datos.

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 estos mismos. *(No podemos conservar datos de socios que se han dado de baja, a no ser que lo especifiquemos expresamente en la ficha de petición de datos, en ese caso deberemos de delimitar hasta cuando los conservaremos antes de eliminarlos)*.

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.

SITUACIONES FRECUENTE EN LAS AMPAS

¿Se puede crear un grupo de WHATS APP o similar con los socios?
Se puede siempre que se haya recogido su consentimiento, para ello lo más adecuado es tener dicha autorización en el documento donde se recogen los datos.

¿Se pueden grabar imágenes del alumnado y difundirlas a través de aplicaciones de mensajería para enviarlas a las familias?
No se puede sino se cuenta con la autorización adecuada. Sólo en aquellos casos en los que el interés superior de los menores estuviera comprometido, accidentes o indisposiciones, y con la finalidad de informar y tranquilizar a las familias, se podrían captar imágenes y enviarlas a los padres.

¿Pueden publicarse las listas de alumnado o asociados?
Sólo en el caso que exista un procedimiento de concurrencia competitiva en el que se valoran y puntúan determinadas circunstancias.

¿Puede facilitarse información que tenga el AMPA del alumnado o asociados?
Sólo a los padres, madres, tutores o tutoras que ostenten la patria y potestad, nunca a otros familiares, salvo que estuvieren autorizados por aquellos y que claramente constase esa autorización.

¿Pueden las AMPAS grabar imágenes del alumnado durante las actividades extraescolares?
Siempre debemos disponer del consentimiento de los interesados o de sus padres si este es menor.

Si los padres, madres o tutores se niegan a que se tomen imágenes de su hijo/a en un acto abierto a las familias, realizado por el AMPA, ¿se ha de cancelar dicho evento?
No. Hay que informar a madres, padres y tutoras que la toma de fotografías y videos es posible como actividad familiar, sólo para uso personal y doméstico, que está excluida de la aplicación de la normativa de protección de datos.
Es conveniente advertir a los asistentes a los eventos que se pueden grabar imágenes para uso personal, familiar o bien de amistad.

¿Pueden publicarse en la web del AMPA fotografías o videos del alumnado?
Sólo si se cuenta con el consentimiento del alumno/a o bien de su padre, madre o tutor si el alumno es menor de 14 años. También puede pixelarse la imagen para evitar que el alumno o alumna pueda ser identificado.

(NOMBRE DEL AMPA)

DATOS

NOMBRE DEL AMPA .....

NIF: .....

DIRECCIÓN: .....

TELÉFONO: ..... CORREO ELECTRÓNICO: .....

Que, de acuerdo con lo que establece el 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), en nombre de *(NOMBRE DEL AMPA)* la información que nos facilita con el fin de prestarles el servicio solicitado, **PONER EL MOTIVO,** *(ejemplo, realizar tareas propias de gestión administrativa de la Asociación para mandar información a socios/as acerca de actividades realizadas por la AMPA)***.** Los datos proporcionados se conservarán mientras se mantenga la relación con nuestra Asociación o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Los datos podrán ser cedidos, como encargados de tratamiento, a las empresas *(poner nombre de las empresas)* que se contraten para realizar actividades extraescolares.

Usted tiene derecho a obtener confirmación sobre si en la **NOMBRE DEL AMPA** estamos tratando sus datos personales, por tanto, tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Asimismo, solicito su autorización *para (se puede poner aquí lo de ofrecer productos, autorización para el tema de utilización de imágenes y videos, siempre poniendo donde se van a utilizar, etc.)*

SÍ ☐

NO ☐

En _____, a ___ de _____ de 20_____

Firmado

ANEXO 2

(NOMBRE DEL AMPA)

SOLICITUD DE ACCESO A DATOS PERSONALES

NOMBRE:		**APELLIDOS:**	
DNI:			
NOMBRE Y APELLIDOS DEL REPRESENTANTE:			
DIRECCIÓN COMPLETA A EFECTOS DE NOTIFICACIÓN			
RESPONSABLE DEL FICHERO:	*(NOMBRE DEL AMPA)*		

SOLICITO:

Que, de acuerdo con lo que establece el 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), me informen de los datos relativos a mi persona que trata *(NOMBRE DEL AMPA) (marcar la opción escogida)*:

- ☐ Visualización en pantalla
- ☐ Escrito
- ☐ Fotocopia
- ☐ Correo electrónico
- ☐ Otros: .....

Documentación que se acompaña (marcar lo que proceda):

- ☐ Copia del DNI o pasaporte
- ☐ Título que acredita la representación
- ☐ Otra documentación: .....

En _____, a ___ de _____ de 20_____

Firmado

ANEXO 3

(NOMBRE DEL AMPA)

SOLICITUD DE RECTIFICACIÓN DATOS PERSONALES

NOMBRE:		**APELLIDOS:**	
DNI:			
NOMBRE Y APELLIDOS DEL REPRESENTANTE:			
DIRECCIÓN COMPLETA A EFECTOS DE NOTIFICACIÓN			
RESPONSABLE DEL FICHERO:	*(NOMBRE DEL AMPA)*		

SOLICITO:

Que, de acuerdo con lo que establece el 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), solicito rectifiquen los datos relativos a mi persona que trata *(NOMBRE DEL AMPA)* ..... *(motivo de la rectificación):*

Dato incorrecto: .....

Dato correcto: .....

Documentación que se acompaña (marcar lo que proceda):

☐ Copia del DNI o pasaporte

☐ Título que acredita la representación

☐ Documentación acreditativa: .....

En _____, a ___ de _____ de 20____

Firmado

ANEXO 4

(NOMBRE DEL AMPA)

SOLICITUD DE SUPRESIÓN-CANCELACIÓN A DATOS PERSONALES

NOMBRE:		**APELLIDOS:**	
DNI:			
NOMBRE Y APELLIDOS DEL REPRESENTANTE:			
DIRECCIÓN COMPLETA A EFECTOS DE NOTIFICACIÓN			
RESPONSABLE DEL FICHERO:	*(NOMBRE DEL AMPA)*		

SOLICITO:

Que, de acuerdo con lo que establece el 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), solicito supriman o cancelen los datos referentes a mi persona que contienen sus ficheros o que sean objeto de tratamiento, y que se relacionan a continuación dado que ..... *(motivo de la cancelación)*.

Datos que hay que suprimir o cancelar: .....

Documentación que se acompaña (marcar lo que proceda):

- ☐ Copia del DNI o pasaporte
- ☐ Título que acredita la representación
- ☐ Documentación acreditativa: .....

En _____, a ___ de _____ de 20_____

Firmado

ANEXO 5

(NOMBRE DEL AMPA)

SOLICITUD OPOSICIÓN A DATOS PERSONALES

NOMBRE:		**APELLIDOS:**	
DNI:			
NOMBRE Y APELLIDOS DEL REPRESENTANTE:			
DIRECCIÓN COMPLETA A EFECTOS DE NOTIFICACIÓN			
RESPONSABLE DEL FICHERO:	NOMBRE DEL AMPA		

SOLICITO:

Que, de acuerdo con lo que establece el 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), cesen en el tratamiento, *(describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)*, a los datos referentes a mi persona que contienen sus ficheros o que sean objeto de tratamiento.

Documentación que se acompaña (marcar lo que proceda):

☐ Copia del DNI o pasaporte

☐ Título que acredita la representación

☐ Documentación acreditativa: _____

En _____, a ___ de _____ de 20____

Firmado

ANEXO 6

(NOMBRE DEL AMPA)

RENOVACIÓN AMPA _____ **Curso 2018/2019**

FORMULARIO DE ALTA O DE VARIACIÓN DE DATOS DE SOCIOS

(Entregar en el sobre de matrícula o depositar en cualquiera de los buzones de la Ampa. Marcar lo que proceda. Los datos de los componentes de la unidad familiar (padre y madre) son importantes para la elaboración del censo de asociados).

CUOTA ANUAL: _____

N.º DE SOCIO: _____

SOCIO TITULAR (Los datos señalados con (*) son obligatorios):

Fecha (*): ___ / ___ / _____

Padre/madre 1º (*): _____

NIF (*): _____

CÓNYUGE: _____

Domicilio (*): _____

Teléfono domicilio: _____

Teléfono móvil: _____

Correo electrónico: _____

	NOMBRE DE LOS NIÑOS/AS	FECHA NACIMIENTO	CURSO
1	_____	_____ / _____ / _____	
2	_____	_____ / _____ / _____	
3	_____	_____ / _____ / _____	
4	_____	_____ / _____ / _____	

Número de cuenta bancaria (20 dígitos):

NOMBRE Y APELLIDOS DEL TITULAR DE LA CUENTA:				
IBAN	**ENTIDAD**	**OFICINA**	**DC**	**N.º DE CUENTA**
FIRMA TITULAR:				

SI NO DESEAS RECIBIR LAS COMUNICACIONES POR CORREO ELECTRÓNICO MARCA ESTA CASILLA. ☐

Que, de acuerdo con lo que establece el 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), en nombre de *(NOMBRE DEL AMPA)* la información que nos facilita con el fin de prestarles el servicio solicitado, *(poner el motivo, por ejemplo, realizar tareas propias de gestión administrativa de la Asociación para mandar información a socios/as acerca de actividades realizadas por la AMPA, pagos y cobros)*. Los datos proporcionados se conservarán mientras se mantenga la relación con nuestra Asociación o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Los datos podrán ser cedidos, como encargados de tratamiento, a las empresas *(poner nombre de las empresas)* que se contraten para realizar actividades extraescolares.

Usted tiene derecho a obtener confirmación sobre si en la *(NOMBRE DEL AMPA)* estamos tratando sus datos personales, por tanto, tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Asimismo, solicito su autorización *para (se puede poner aquí lo de ofrecer productos, autorización para el tema de utilización de imágenes y videos, siempre poniendo donde se van a utilizar, etc.).*

SÍ ☐ NO ☐

En _____, a _____ de _____ de _____

(NOMBRE DEL AMPA)

FICHA DE INSCRIPCIÓN EN LA ACTIVIDAD DE _____ Curso 2018/2019

FORMULARIO DE ALTA

(Entregar en el sobre de matrícula o depositar en cualquiera de los buzones de la Ampa. Marcar lo que proceda. Los datos de los componentes de la unidad familiar (padre y madre) son importantes para la elaboración del censo de asociados).

FECHA: _____

DATOS DEL ALUMNO/A (Los datos señalados con (*) son obligatorios):

NOMBRE Y APELLIDOS (*):

_____

EDAD (*): _____ CURSO (*): _____ SE QUEDA A COMEDOR (*): SÍ ☐ NO ☐

FECHA (*): ____ / ____ / _____

PADRE/MADRE 1º (*): _____

NIF (*): _____

DOMICILIO (*): _____

TELÉFONO MÓVIL: _____

FIRMA TITULAR:	

SI NO DESEAS RECIBIR LAS COMUNICACIONES POR CORREO ELECTRÓNICO MARCA ESTA CASILLA. ☐

Que, de acuerdo con lo que establece el 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), en nombre *de(NOMBRE DEL AMPA)* la información que nos facilita con el fin de prestarles el servicio solicitado, *(poner el motivo, por ejemplo, realizar tareas propias de gestión administrativa de la Asociación para mandar información a socios/as acerca de actividades realizadas por la AMPA, pagos y cobros)*. Los datos proporcionados se conservarán mientras se mantenga la relación con nuestra Asociación o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Los datos podrán ser cedidos, como encargados de tratamiento, a las empresas *(poner nombre de las empresas)* que se contraten para realizar actividades extraescolares.

Usted tiene derecho a obtener confirmación sobre si en la *(NOMBRE DEL AMPA)* estamos tratando sus datos personales, por tanto, tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Asimismo, solicito su autorización *para (se puede poner aquí lo de ofrecer productos, autorización para el tema de utilización de imágenes y videos, siempre poniendo donde se van a utilizar, etc.)*

DOCUMENTO DE SEGURIDAD

FECHA VERSIÓN DEL DOCUMENTO DE SEGURIDAD	*(fecha de alta)*
VERSIÓN DEL DOCUMENTO DE SEGURIDAD	*(001)*

DOCUMENTO DE SEGURIDAD DE LOS FICHEROS DE LA *(NOMBRE DEL AMPA)*

AVISO DE CONFIDENCIALIDAD

A este documento, así como al resto de documentación y de informaciones relacionadas con las medidas de seguridad de los ficheros de la *(NOMBRE DEL AMPA)*, sólo tienen acceso las personas designadas en este mismo documento, sin perjuicio que el cumplimiento de las obligaciones derivadas de la regulación del derecho a la protección de datos de carácter personal o de otras normativas aplicables implique el acceso a este documento por parte de terceros.

ESTRUCTURA DEL DOCUMENTO DE SEGURIDAD

Este documento y sus Anexos recogen las medidas de carácter técnico y organizativo necesarias para garantizar la seguridad de los datos y de los tratamientos relacionados con los ficheros responsabilidad de *(NOMBRE DEL AMPA)*. Estas medidas sirven para evitar la alteración, la pérdida, el tratamiento o el acceso no autorizado a los datos que contienen y garantizar su disponibilidad.

- **PARTE GENERAL.**
  - ***1**. Ámbito de aplicación del documento.*
  - ***2**. Normativa aplicada y medidas de seguridad aplicables.*
  - ***3**. Funciones y obligaciones del personal.*
  - ***4**. Estructura de los ficheros y descripción de los sistemas de tratamiento.*
  - ***5.** Gestión de incidencias.*
  - ***6.** Copias de seguridad.*
  - ***7.** Gestión de soportes y documentos.*
  - ***8.** Destrucción de información y reutilización de soportes.*
  - ***9.** Auditoría.*
  - ***10.** Revisión del documento de seguridad.*
  - ***11.** Anexo medidas de seguridad.*

1. ÁMBITO DE APLICACIÓN DEL DOCUMENTO.

Este documento de seguridad ha sido elaborado por *(NOMBRE DEL AMPA)*, que es responsable de los ficheros que se detallan a continuación:

DENOMINACIÓN DEL FICHERO	NIVEL DE SEGURIDAD	SISTEMA DE TRATAMIENTO
(nombre del fichero)	BÁSICO	MIXTO

Este documento se tiene que mantener permanentemente actualizado y cualquier modificación relevante tiene que comportar su revisión y, si procede, la modificación parcial o total.

2. NORMATIVA APLICADA Y MEDIDAS DE SEGURIDAD APLICABLES.

En la elaboración de este documento de seguridad se ha tenido en cuenta la normativa siguiente:

- 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)

Son de aplicación a los diferentes ficheros a que se refiere este documento de seguridad las medidas de seguridad previstas en el RGPD y las que se concretan en este documento, de acuerdo con el nivel de seguridad que se describe para cada uno de ellos en el apartado 1 de este documento.

Las medidas que se describen en este documento para cada nivel de seguridad son de carácter acumulativo, es decir, que en cada nivel se tienen que aplicar no sólo las medidas indicadas específicamente para este nivel, sino también las que corresponden a los niveles inferiores.

3. FUNCIONES Y OBLIGACIONES DE LAS PERSONES AUTORIZADAS A TRATAR LOS DATOS.

Las personas que tengan acceso o que traten los datos contenidos en los ficheros de la *(NOMBRE DEL AMPA)* tienen que conocer y observar las medidas de seguridad y obligaciones relacionadas establecidas en este documento de seguridad.

Con este objetivo, se les tiene que entregar una copia del documento de seguridad vigente, con la advertencia que se trata de un documento confidencial y que tienen que mantener reserva sobre su contenido. Para acceder a los datos, hace falta que hayan firmado la recepción del documento.

Obligaciones de carácter general para las personas con acceso a los datos de los ficheros:

1. Conocer y cumplir, en aquello que les sea de aplicación, lo que prevé este documento de seguridad.
2. Notificar a **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)* cualquier incidencia que pueda afectar a la seguridad de los datos.
3. Guardar secreto y confidencialidad sobre los datos personales de los ficheros.

El Anexo **REG001** recoge la lista de las personas a quienes se ha entregado el documento de seguridad, con la fecha y la firma de recepción.

El personal ajeno a la *(NOMBRE DEL AMPA)*, con acceso a los datos, está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio así como a las previsiones específicas incluidas en este documento de seguridad y las que se incluyan en el acuerdo o contrato de encargo del tratamiento.

En el caso de incumplimiento de lo que se prevé en este documento, la *(NOMBRE DEL AMPA)*, se reserva el derecho de iniciar las acciones legales que considere más adecuadas para proteger sus intereses o los de terceros.

3.1. Control de acceso a datos.

El personal sólo puede acceder a los datos y a los recursos necesarios para ejercer sus funciones. Las personas autorizadas a acceder a los datos de los ficheros y las operaciones que pueden realizar cada uno de ellos figuran en el Anexo **INF002**. Las personas con acceso a los datos sólo pueden hacer uso de ellos en relación con las funciones que tienen atribuidas.

Para que otras personas que no figuran en este documento de seguridad puedan acceder a la información, hay que contar con la autorización del responsable del fichero o del responsable de seguridad.

3.2. Identificación y autenticación.

Cada usuario autorizado a acceder a los datos de los ficheros tiene asignado un código de usuario personal y una palabra de paso o contraseña que lo identifica de forma inequívoca y le permite autenticarse en los equipos necesarios para acceder a la información.

Corresponde a **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*, dar de alta y de baja a los usuarios del sistema y proporcionarles el código de usuario y la palabra de acceso asignada que se dará directamente en sobre cerrado. La palabra de acceso otorgada y sus modificaciones se tienen que almacenar de manera cifrada.

Las palabras de paso o contraseñas asignadas tienen que reunir las características siguientes: una longitud mínima de ocho caracteres y la combinación de letras, números, mayúsculas, minúsculas y, si el sistema lo permite, símbolos.

Las palabras de paso o contraseñas se tienen que modificar la primera vez que el usuario accede al ordenador y antes de acceder o tratar los datos incluidos en los ficheros. Asimismo, cada usuario tiene que modificar su palabra de acceso o contraseña cada seis meses.

3.3. Responsable de seguridad.

Se designa como responsable de seguridad a **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA),* que se encarga de coordinar y controlar las medidas establecidas en este documento de seguridad en relación con el único fichero, calificadas de nivel bajo.

En ningún caso la designación supone la exoneración de la responsabilidad que corresponde a la *(NOMBRE DEL AMPA)* como responsable del fichero.

La designación se hace por un periodo de **dos años**. Transcurrido este plazo, se puede nombrar a la misma persona como responsable de seguridad u otra diferente.

El responsable de seguridad tiene que hacer controles periódicos, como mínimo cada **seis meses**, para verificar el cumplimiento de lo que dispone este documento de seguridad.

3.4. Prestación de servicios por terceros con acceso a datos.

La prestación de servicios por terceras personas o entidades, que comporta el acceso a datos personales de los ficheros o de los sistemas de que es responsable la *(NOMBRE DEL AMPA)*, requiere la suscripción del contrato o el acuerdo de encargo y se considera un encargado de tratamiento.

En el Anexo **INF005**, se relacionan los terceros que actúan como encargados del tratamiento por cuenta de la *(NOMBRE DEL AMPA)*, con indicación de si los datos necesarios para prestar los servicios se tratan en los locales de la *(NOMBRE DEL AMPA)* o bien en los del encargado de los ficheros o tratamientos afectados por el encargo, y del contrato o acuerdo de encargo suscrito y su vigencia.

El encargado del tratamiento tiene que guardar secreto y confidencialidad sobre los datos personales de los ficheros a los cuales tiene acceso para prestar el servicio encargado.

3.4.1. Tratamiento de los datos en los locales de la (NOMBRE DEL AMPA).

Si, de conformidad con el contrato o el acuerdo de encargo suscrito, el servicio se presta en los locales de la *(NOMBRE DEL AMPA)*, el acceso del encargado del tratamiento a los datos de los ficheros y los sistemas se debe hacer con los recursos y los sistemas de información que facilite la *(NOMBRE DEL AMPA)*.

El personal del encargado del tratamiento tiene que cumplir las medidas de seguridad previstas en este documento de seguridad, de conformidad con el nivel de seguridad que se describe para cada uno de los ficheros en el apartado 1 de este documento. A este efecto, se les tiene que entregar una copia íntegra del documento de seguridad vigente y dejar constancia en el Anexo **REG001**.

Los datos de los ficheros a que se accede para prestar el servicio no pueden salir fuera de los locales de la *(NOMBRE DEL AMPA)*.

Para que los datos se puedan tratar fuera de los locales de la *(NOMBRE DEL AMPA)*, así como para incorporarlos a dispositivos portátiles, hace falta que la autorización conste en el Anexo **INF002** de este documento de seguridad. En estos casos, hay que garantizar el nivel de seguridad correspondiente.

Una vez cumplida la prestación del servicio, el encargado del tratamiento tiene que destruir o devolver las copias de los datos y, si procede, los soportes donde constan, según lo que se establece en el Anexo **INF005** de este documento de seguridad.

Si se ha establecido que el encargado tiene que devolver al responsable de los ficheros, o a otro encargado que se haya designado, los datos personales y, si procede, los soportes donde constan, el encargado del tratamiento garantiza que el retorno comporta el borrado total de los datos de sus equipos informáticos utilizados para prestar el servicio, para impedir así su reutilización.

Si se ha establecido que los datos personales y, si procede, los soportes donde constan, se tienen que destruir, la destrucción se tiene que hacer de acuerdo con el procedimiento establecido en el apartado 8 de este documento de seguridad y, en cualquier caso, se tiene que certificar por escrito. Este certificado se tiene que transmitir a la *(NOMBRE DEL AMPA)*, lo antes posible.

El acceso remoto del encargado del tratamiento a datos, cuando así consta en el contrato o acuerdo de encargo suscrito, se hace mediante el sistema de autenticación de usuarios registrados establecido en el apartado 3.2 de este documento de seguridad.

El encargado del tratamiento tiene que poner en conocimiento de **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*, cualquier incidencia que pueda afectar a la seguridad de los datos, de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

3.4.2. *Tratamiento de los datos en los locales del encargado del tratamiento:*

Cuando, de conformidad con el contrato o acuerdo de encargo suscrito, los datos de los ficheros de los cuales es responsable la *(NOMBRE DEL AMPA)*, necesarios para prestar el servicio, se tratan en los locales del encargado del tratamiento, y exclusivamente con sus sistemas, éste se compromete a elaborar un documento de seguridad o bien a completar su propio documento de seguridad, si procede, con la indicación de:

- Ficheros afectados por la prestación del servicio.
- Responsable de los ficheros.
- Condiciones del encargo, en especial las medidas de seguridad establecidas en el contrato o el acuerdo de encargo.
- Periodo de vigencia del encargo.

Los datos de los ficheros a que se accede para prestar el servicio no pueden salir fuera de los locales del encargado del tratamiento. En caso de que sea necesario cambiar los locales donde se tratan, el encargado lo tiene que comunicar previamente a la *(NOMBRE DEL AMPA)*.

Para tratar los datos fuera de los locales del encargado del tratamiento, así como para incorporarlos a dispositivos portátiles, hace falta que conste la autorización en el Anexo **INF002** de este documento de seguridad. En estos casos, hay que garantizar el nivel de seguridad correspondiente.

El encargado del tratamiento tiene que anotar las incidencias de seguridad en su registro de incidencias y tiene que poner en conocimiento de **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*, de forma inmediata, cualquier incidencia que se produzca durante la ejecución del contrato que pueda afectar a la seguridad de los datos, de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

En dicho caso, el responsable del tratamiento tiene la obligación de notificar los fallos de seguridad que se produzcan en su organización a la Agencia Española de Protección de Datos (AEPD) en un plazo de **72 horas**. El responsable del tratamiento debe contar con un sistema efectivo para realizar el reporte a la AEPD o para comunicar el fallo a los afectados si existe algún riesgo para sus derechos.

El encargado del tratamiento se tiene que someter a las auditorías de cumplimiento de la normativa de protección de datos decididas por la *(NOMBRE DEL AMPA)*, al inicio de la prestación, como mínimo cada dos años y, en cualquier caso, siempre que se produzcan modificaciones sustanciales en los sistemas de información.

Una vez cumplida la prestación del servicio, el encargado del tratamiento tiene que destruir, entregar a un tercero o devolver las copias de los datos y, si procede, los soportes donde constan, de acuerdo con lo que se establece en el Anexo **INF005** de este documento de seguridad. Todo esto, sin perjuicio de que pueda guardar una copia, bloqueada, para hacer frente a las posibles responsabilidades derivadas del encargo.

Si se ha establecido que el encargado tiene que devolver los datos personales y, si procede, los soportes donde constan, al responsable de los ficheros o a otro encargado que haya designado, el encargado del tratamiento garantiza que el retorno comporta el borrado total de los datos de sus equipos informáticos utilizados para prestar el servicio.

Si se ha establecido que los datos personales y, si procede, los soportes donde constan se tienen que destruir, la destrucción se tiene que certificar por escrito. Este certificado se tiene que transmitir a la *(NOMBRE DEL AMPA)*, lo antes posible.

3.5. Prestación de servicios por terceros sin acceso a datos.

El prestador del servicio se tiene que comprometer a poner en conocimiento de su personal las medidas que se detallan a continuación y a conservar la acreditación del cumplimiento de este deber.

El personal de las empresas contratadas para prestar servicios que no comportan el tratamiento de datos personales no puede acceder a los datos que figuran en archivos, documentos, ficheros y sistemas de información de la *(NOMBRE DEL AMPA)*.

El personal de la empresa prestadora del servicio que tiene que acceder a los locales de la **NOMBRE AMPA**, ha de contar con el permiso para el acceso a los locales.

En el Anexo **INF006** se relacionan los prestadores de servicios de la *(NOMBRE DEL AMPA)*, sin acceso a datos personales.

El acceso a los lugares en que están ubicados los servidores de la *(NOMBRE DEL AMPA)*, se tiene que hacer cuando esté presente personal de la *(NOMBRE DEL AMPA)*.

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el documento Anexo **INF002**.

El prestador del servicio tiene que poner en conocimiento de **el/la Presidente/Presidenta** de la *(NOMBRE DEL AMPA)*, de manera inmediata, cualquier incidencia que se produzca durante la ejecución del servicio que pueda afectar a la integridad o la confidencialidad de los datos personales tratados por la *(NOMBRE DEL AMPA)*, de conformidad con el procedimiento establecido en el apartado 5 de este documento de seguridad.

En dicho caso, el responsable del tratamiento tiene la obligación de notificar los fallos de seguridad que se produzcan en su organización, a la Agencia Española de Protección de Datos (AEPD) en un plazo de **72 horas**. El responsable del tratamiento debe contar con un sistema efectivo para realizar el reporte a la AEPD o para comunicar el fallo a los afectados si existe algún riesgo para sus derechos.

Esta circunstancia se tiene que anotar en el registro de incidencias.

En caso de acceso accidental a datos personales, el personal del prestador del servicio está obligado a guardar secreto, incluso una vez finalizada la relación contractual. En ningún caso puede utilizar los datos ni revelarlos a terceros.

3.6. Delegación de autorizaciones y funciones de control.

En el Anexo **INF004** se recoge una relación de las personas a las cuales el responsable del fichero delega las autorizaciones que se mencionan.

4. ESTRUCTURA DE LOS FICHEROS Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO.

La estructura de los ficheros se detalla en el Anexo **INF003**.

El sistema de tratamiento de los datos de los ficheros es parcialmente automatizado, ya que hay datos en ficheros informáticos, según las características descritas en los Anexos **INF001** e **INF003,** y también se dispone de información en formato papel, ya sea como soporte a la recogida de datos o para las salidas impresas del sistema informático.

Las medidas de seguridad implantadas son las del nivel que se indica en el apartado 1 de este documento para cada fichero, previstas en la normativa de protección de datos para los tratamientos automatizados y no automatizados.

Los datos de los ficheros pueden ser objeto de cualquier operación relacionada con su finalidad. Por lo tanto, de acuerdo con lo que se establece en el Anexo **INF002**, los usuarios autorizados pueden hacer operaciones de recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, y también, si procede, la cesión a terceros como resultado de comunicaciones, consultas, interconexiones o transferencias de datos.

Estas operaciones se realizan tanto en relación a soportes automatizados como no automatizados, en cada caso adaptadas al sistema concreto de tratamiento.

4.1. Sistema de información.

El sistema de información de los ficheros se basa en ficheros almacenados en un PC, que se almacenan en forma de BBDD, y en copias de seguridad que se encuentran en pen drive, donde se recogen los datos de **(***COLECTIVOS INTERESADOS, ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias...)*

El sistema de información de los ficheros se complementa con un archivo físico de papel, donde de manera estructurada se archivan los documentos relacionados con los datos recogidos de (*COLECTIVOS INTERESADOS, ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias...)*

4.2. Copias de trabajo de documentos o ficheros temporales.

Una copia de trabajo parcial o total de los ficheros o de documentos en papel, para una tarea concreta o auxiliar relacionada con las finalidades de los ficheros, se considera un "fichero temporal". Le es de aplicación el nivel de seguridad que corresponda de acuerdo con los criterios establecidos en el RGPD y lo que establece este documento de seguridad.

Una vez finalizada la tarea temporal, la copia de trabajo del fichero o de la documentación se tiene que destruir, según el procedimiento que prevé el apartado 8 de este documento.

4.3. Régimen de trabajo fuera de los locales de la *(NOMBRE DEL AMPA)*

Se pueden hacer los tratamientos de datos personales de los ficheros fuera de los locales de la *(NOMBRE DEL AMPA),* en los supuestos siguientes: en **Asambleas y Juntas Directivas**.

Se pueden utilizar dispositivos portátiles en los supuestos siguientes: en **Asambleas y Juntas Directivas**.

Las personas autorizadas a este efecto son las que figuran en el Anexo **INF002**.

4.4. Acceso a datos a través de redes de comunicaciones.

Se puede acceder a través de redes de comunicaciones a los ficheros siguientes *(poner nombre del fichero y ubicación del mismo)*.

El acceso a los ficheros a través de redes de comunicaciones se tiene que hacer con medidas que garanticen un nivel de seguridad equivalente al exigido para los accesos en modo local.

5. GESTIÓN DE INCIDENCIAS.

Se considera "incidencia de seguridad" cualquier incumplimiento de la normativa aplicable o de este documento de seguridad, así como cualquier otra anomalía que afecte o pueda afectar a la seguridad de los datos personales de la *(NOMBRE DEL AMPA)*.

Las personas relacionadas en el Anexo **INF002** tienen que comunicar lo antes posible la incidencia a **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*.

Esta comunicación se tiene que hacer oral, por escrito, correo electrónico o culaquier otro medio que se considere oportuno. **El/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)* gestiona las comunicaciones recibidas, las valora y adopta, si procede, las medidas oportunas para corregir la situación detectada.

El/la Presidente/Presidenta de la *(NOMBRE DEL AMPA)* tiene que anotar en el registro de incidencias, (ver documento Anexo **REG002**), los datos siguientes relacionados con la incidencia detectada:

1. Tipo de incidencia
2. Momento en que se ha producido y detectado
3. Quién la ha notificado
4. A quién la ha comunicado
5. Consecuencias
6. Medidas correctoras adoptadas o que se proponen

El responsable del tratamiento tiene la obligación de notificar los fallos de seguridad que se produzcan en su organización, a la Agencia Española de Protección de Datos (AEPD), en un plazo de **72 horas**. El responsable del tratamiento debe contar con un sistema efectivo para realizar el reporte a la AEPD o para comunicar el fallo a los afectados si existe algún riesgo para sus derechos.

6. COPIAS DE SEGURIDAD Y RECUPERACIÓN.

6.1. Copia de seguridad.

Se tiene que hacer una copia de seguridad semanal de los ficheros, a menos que los datos no se hayan modificado durante el periodo mencionado.

Este proceso consiste en copiar los ficheros en un dispositivo externo, de acuerdo con el procedimiento siguiente:

El proceso de copia de seguridad tiene que permitir garantizar la reconstrucción de los ficheros al estado que tenían en el momento de producirse una eventual pérdida o destrucción de los datos.

La copia de seguridad la tiene que hacer **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*.

Cada seis meses **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)* tiene que verificar que las copias se hacen correctamente y que se pueden restaurar. Para hacerlo, tiene que aplicar los procedimientos de copia y restauración sin afectar a los datos reales. Los ficheros resultantes se tienen que suprimir una vez hechas las verificaciones.

Si entre la fecha en que se hizo la última copia de seguridad y la fecha en que es necesario hacer la restauración, la información se ha modificado y se puede recuperar manualmente a partir de documentación en papel, esta circunstancia se tiene que hacer constar en el registro de incidencias con el máximo detalle posible.

Si hace falta modificar el hardware o bien sustituir los ordenadores, o trasladar los datos a otro tipo de fichero, antes se tiene que hacer una copia de seguridad.

Se tiene que evitar hacer pruebas con datos reales, antes de implantar o modificar los sistemas de información. Si no es posible, se tiene que hacer previamente una copia de seguridad, se tiene que asegurar el nivel de seguridad correspondiente al tratamiento realizado y anotar las pruebas en este documento de seguridad.

En el Anexo **REG003** se tiene que anotar la fecha y la hora de ejecución de cada copia de seguridad, la persona que lo ha hecho y las observaciones relativas al proceso.

6.2. Recuperación.

Si hay que utilizar la copia de seguridad para recuperar la información, se tiene que seguir el procedimiento de copia a la inversa, copiando la información del dispositivo externo de almacenamiento a la carpeta del ordenador donde tiene que quedar ubicado el fichero.

Si la información de recuperación se introduce manualmente, hay que dejar constancia en el registro de incidencias.

7. GESTIÓN DE SOPORTES Y DOCUMENTOS.

Los soportes con datos de carácter personal se deben identificar con los tipos de información que contienen, se deben inventariar y se deben almacenar en el lugar de acceso restringido, que consta en el Anexo **REG004,** al cual sólo tienen acceso las personas que se relacionan en el Anexo mencionado.

En el inventario de soportes constan las personas autorizadas para acceder a cada uno de los soportes.

En caso de que, por razón de urgencia o fuerza mayor, tenga que acceder personal no autorizado, es necesario estar presente personal de la *(NOMBRE DEL AMPA)*.

Si hay que traspasar los datos a un soporte externo (p. ej. disco duro externo, memoria USB, CD o DVD, etc.) fuera del equipo donde se tratan habitualmente, este soporte se tiene que etiquetar con el **NOMBRE FICHERO y dd/mm/aaaa**, de manera que se pueda reconocer con facilidad el contenido y la fecha de copiado de los datos.

7.1. Dispositivos de almacenamiento de los documentos en papel.

Para guardar los documentos en soporte papel con datos personales se pueden utilizar los elementos de almacenaje siguientes: armarios con llave.

7.2. Criterios de archivo de la documentación en papel.

El archivo de los soportes o de la documentación se tiene que hacer de acuerdo con los criterios y las normas de seguridad previstas en el RGPD.

7.3. Custodia de los documentos en papel.

Cuando la documentación en soporte papel no está depositada en los dispositivos de almacenamiento habituales, circunstancia que sólo se puede dar cuando se está trabajando, la persona que la utiliza tiene que custodiarla e impedir que puedan acceder personas no autorizadas. Hay que tener especial cuidado de no descuidar papeles en la mesa de trabajo o en otros espacios comunes o de libre acceso.

7.4. Salida de soportes y documentos.

En el inventario de soportes constan las autorizaciones de salida de los soportes y documentos, incluidos los contenidos en correos electrónicos o en cualquier dispositivo móvil, fuera de la *(NOMBRE DEL AMPA)* y la persona que la ha autorizado. Tienen que constar, de manera diferenciada, tanto las autorizaciones de salida de soportes y documentos genéricos de procesos periódicos que se prevén en el documento de seguridad, como las autorizaciones de salidas puntuales de soportes y documentos hechas específicamente por el responsable de los ficheros.

La autorización de la salida de los soportes se tiene que hacer como indica el Anexo **INF007**.

Durante el traslado físico de los soportes que contienen datos personales se tienen que aplicar las medidas siguientes para evitar la sustracción, el acceso indebido o la pérdida de la información: llevar la información cifrada.

La persona que transporta el soporte es la responsable de custodiarlo. Por lo tanto, tiene que actuar con la diligencia necesaria para aplicar estas medidas y evitar incidentes con los datos. En todo caso, **el/la Presidente/Presidenta** *(NOMBRE DEL AMPA)* puede dar instrucciones concretas de protección cuando lo considere conveniente. Esta circunstancia tiene que quedar recogida en el inventario de soportes.

7.5. Copia o reproducción de los documentos en papel.

Las copias o la reproducción de documentos con datos personales de ficheros de nivel alto sólo se pueden hacer bajo el control del personal autorizado que figura en el Anexo **INF002**.

Las copias rechazadas se tienen que destruir, de manera que se imposibilite el acceso posterior a la información que contienen, de acuerdo con lo que se describe en el apartado 8 de este documento.

8. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES.

8.1. Información en soportes digitales.

Los soportes digitales -tipo disco duro externo o interno, o memoria flash con interfaz USB- que se tengan que rechazar o reutilizar para otras finalidades se tienen que formatear de nuevo.

Esto se puede hacer mediante el programa **ERASER**.

La función simple de borrar o suprimir un fichero no es suficiente, considerando que no es un procedimiento seguro y que la información podría ser recuperada por terceros.

Los dispositivos tipo CD o DVD, ante la imposibilidad de hacer uno borrado "seguro", se tienen que destruir físicamente mediante la destructora habilitada en el local de la *(NOMBRE DEL AMPA)* de manera que quede inutilizable.

Para los casos en que no se tiene que rechazar el soporte o reutilizarlo con otra finalidad, sino sólo borrar los ficheros o informaciones que contienen los ordenadores, hay que utilizar la opción "eliminar" o "suprimir" y, a continuación, vaciar la carpeta de los mensajes eliminados o la papelera de reciclaje del ordenador.

8.2. Información en soporte papel.

Se pueden rechazar documentos en soporte papel que incluyan datos personales, de acuerdo con el sistema siguiente: utilizar la destructora de papel ubicada en la *(NOMBRE DEL AMPA)*.

Se prohíbe tirar documentos que contengan información personal en las papeleras o similares así como reutilizarlos.

9. AUDITORÍA.

Solo es necesario en los ficheros de NIVEL MEDIO Y ALTO.

10. REVISIÓN DEL DOCUMENTO DE SEGURIDAD.

Este documento de seguridad se tiene que adecuar a las disposiciones vigentes en materia de seguridad de los datos de carácter personal y se tiene que mantener permanentemente actualizado mediante una revisión periódica bienal.

También se tiene que revisar y actualizar cuando se produzcan cambios relevantes en los sistemas de tratamiento o en la información tratada. Se consideran cambios relevantes los que pueden repercutir en el cumplimiento de las medidas de seguridad implantadas.

La versión original y actualizada de este documento de seguridad está en poder y bajo el control de **el/la Presidente/Presidenta de la** *(NOMBRE DEL AMPA)*.

La tabla siguiente recoge las modificaciones y actualizaciones de que ha sido objeto este documento de seguridad, así como las revisiones periódicas realizadas a fecha de hoy.

CONTROL DE VERSIONES DEL DOCUMENTO DE SEGURIDAD			
Versión	**Fecha**	**Contenido actualizado/revisión**	**Revisado por**
XXX	dd/mm/aaaa	..... *(indicar el contenido actualizado o revisado)*	..... *(indicar la persona física, área o departamento que lo ha revisado o actualizado)*

CONTROL DE VERSIONES DE LOS ANEXOS				
Anexo	**Versión**	**Fecha**	**Contenido actualizado/revisión**	**Revisado por**
XXX	XXX	dd/mm/aaaa	..... *(indicar el contenido actualizado o revisado)*	..... *(indicar la persona física, área o departamento que lo ha revisado o actualizado)*

11. ANEXO MEDIDAS DE SEGURIDAD.

INFORMACIÓN DE INTERÉS GENERAL.

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud y datos de orientación sexual de las personas, así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS.

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES.

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de dichos datos y serán informados acerca de las correspondientes obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO.

  - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de video vigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.

  - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

  - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

  - No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

  - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- DERECHOS DE LOS TITULARES DE LOS DATOS.

  Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

  - Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.
    Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que se disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL.

  - Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL como, por ejemplo, el robo o acceso indebido a los datos personales, se notificará a la Agencia Española de Protección de Datos en término de 72 horas, acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

- CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEO VIGILANCIA).

  - **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.

  - **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.

  - **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

  - **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes a través un distintivo informativo donde, mediante un pictograma y un texto, se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.

  - **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

  - **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.

  No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

  Para más información puede consultar las guías de videovigilancia de la Agencia Española de Protección de Datos que se encuentran a su disposición en la sección de publicaciones de la web www.agpd.es.

MEDIDAS TÉCNICAS.

- IDENTIFICACIÓN.
  - Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.

- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y de acceso de personas distintas del usuario.

— DEBER DE SALVAGUARDA.

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida posible.

- **MALWARE**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice, en la medida posible, el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- **CORTAFUEGOS O FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.
Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales y la información que trata su empresa, el Instituto Nacional de Ciberseguridad (INCIBE) en su página web www.incibe.es, pone a su disposición herramientas con enfoque empresarial en su sección «Protege tu empresa» donde, entre otros servicios, dispone de:

— Un apartado de formación con un videojuego, retos para respuesta a incidentes y videos interactivos de formación sectorial,

— Un Kit de concienciación para empleados,

— Diversas herramientas para ayudar a la empresa a mejorar su ciberseguridad, entre ellas políticas para el empresario, el personal técnico y el empleado, un catálogo de empresas y soluciones de seguridad y una herramienta de análisis de riesgos.

— Dosieres temáticos complementados con videos e infografías y otros recursos,

— Guías para el empresario,

— Además INCIBE, a través de la Oficina de Seguridad del Internauta, pone también a su disposición herramientas informáticas gratuitas e información adicional que pueden ser de utilidad para su empresa o su actividad profesional.

➢ ANEXOS.

CÓDIGO DOCUMENTO	DESCRIPCIÓN
INF001	Descripción del sistema informático. Características técnicas del hardware y el software.
INF002	Usuarios y autorizaciones de acceso a los datos.
INF003	Estructura de los ficheros.
INF004	Delegación de autorizaciones.
INF005	Encargados del tratamiento.
INF006	Prestadores de servicios sin acceso a datos.
INF007	Autorización salida de soportes.
REG001	Entrega del documento de seguridad.
REG002	Registro de incidencias.
REG003	Registro de copias de seguridad.
REG004	Inventario de soportes.

Anexo INF001

INF001	*Descripción del sistema informático.*
	Características técnicas de hardware y software.

FECHA VERSIÓN DEL ANEXO INF001	*(fecha de alta*
VERSIÓN	*(001)*

Características técnicas de los equipos y programas con los cuales se tratan los datos del fichero.

HARDWARE

Marca y modelo del ordenador:
Número de serie:
Memoria RAM:

Dispositivos de Almacenamiento

Disco duro interno [DISCO_1]	GB
CD grabador	
DVD grabador	
Puertos USB	
Disquetera	
Otros puertos / interfaces externas	*(describirlos)*

Conectividad

Conectado a una red de área local
Interfaz red
Conectado a Internet
Servicio acceso a Internet

Otross dispositivos

Impresora
Escáner

SOFTWARE

Sistema operativo
Antivirus
Cortafuegos
Navegador Internet
Cliente de correo electrónico

Aplicaciones ofimáticas

Tratamiento de textos
Hojas de cálculo
Presentaciones

Otras aplicaciones

(indicar la funcionalidad)	*(indicar nombre y versión)*

Anexo INF002

INF002	*Usuarios y autorizaciones de acceso a los datos*

FECHA VERSIÓN DEL ANEXO INF002	*(fecha de alta)*
VERSIÓN	*(001)*

Relación de usuarios autorizados a acceder a los ficheros con indicación de las operaciones que tienen autorizadas, tanto con respecto a tratamientos automatizados como no automatizados.

Usuario : *(NOMBRE PERSONA)*

Cargo / función : *(PRESIDENTE/A)*

Otros puertos / interfaces externas : *(PUESTO 1)*

Autorizaciones

Consultar

Añadir : SÍ

Modificar : SÍ

Cancelar : SÍ

Suprimir definitivamente : SÍ

Imprimir : SÍ

Copiar : SÍ

Comunicar : SÍ

Desbloquear : SÍ

Supervisar realización copias en papel : SÍ

Operaciones técnicas

Administrar sistema : SÍ

Hacer copias de seguridad : SÍ

Restaurar copias de seguridad : SÍ

Destruir / borrar dispositivos : SÍ

Reutilizar dispositivos : SÍ

Trabajo fuera de los locales de : SÍ

Acceso físico a los equipos : SÍ

(Añadir tantas fichas como sea necesario, una para cada usuario de los ficheros).

Anexo INF003

INF003	*Estructura de los ficheros y descripción de los sistemas de tratamiento*

FECHA VERSIÓN DEL ANEXO INF003	*(fecha de alta)*
VERSIÓN	*(001)*

Identificación del fichero: NOMBRE FICHERO

Sistema de tratamiento: MIXTO

Datos de: COLECTIVOS INTERESADOS - DATOS DE CARACTER IDENTIFICATIVO

(Los colectivos hace referencia a las personas a las que se le van solicitar los datos. Ejemplo: madres, padres, alumnos, alumnas, monitores, monitoras, personal voluntario....)

(Datos de carácter identificativo hace referencia al tipo de datos que se van a solicitar. Ejemplo: nombre. apellidos, dni, dirección, teléfono, correo electrónico, cuenta corriente...)

Anexo INF004

INF004	*Usuarios y autorizaciones de acceso a los datos*

FECHA VERSIÓN DEL ANEXO INF004	*(fecha de alta)*
VERSIÓN	*(001)*

La *(NOMBRE DEL AMPA)* delega las funciones que se relacionan a continuación en las personas siguientes:

PERSONA DELEGADA	**FUNCIÓN**

(indicar las delegaciones que se hagan, como por ejemplo autorizar la salida de dispositivos portátiles; autorizar la destrucción de soportes, revisar las copias de seguridad cada 6 meses; etc.).

Anexo INF005

INF005	*Encargados del tratamiento*

FECHA VERSIÓN DEL ANEXO INF005	*(fecha de alta)*
VERSIÓN	*(001)*

1. Objeto del encargo del tratamiento.

Mediante las presentes cláusulas se habilita a *(nombre de la empresa, NIF/CIF, domicilio, teléfono, correo electrónico…)*, como encargado del tratamiento, para tratar por cuenta de *(NOMBRE DEL AMPA)*, en calidad de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en *(tipo de actividad, por ejemplo, actividades extraescolares)*.

2. Identificación de la información afectada.

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad *(NOMBRE DEL AMPA)* como responsable del tratamiento, pone a disposición de la entidad *(nombre de la empresa)*, la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración

El presente acuerdo tiene una duración de *(periodo de tiempo)*, renovable.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento.

El encargado del tratamiento y todo su personal se obliga a:

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y a través de la dirección de correo electrónico, que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.
Se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías, el número aproximado de interesados afectados y el número aproximado de registros de datos personales afectados.

b) Datos de la persona de contacto para obtener más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

- ✓ Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realice el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- ✓ Destino de los datos

El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento.

Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

En _____, a _____ de _____ de _____

(Firma del encargado de tratamiento) *(Firma del resposable de fichero)*

Anexo INF006

INF006	*Prestadores de servicios sin acceso a datos*

FECHA VERSIÓN DEL ANEXO INF006	*(fecha de alta)*
VERSIÓN	*(001)*

Relación de las personas físicas o jurídicas, públicas o privadas, contratadas por *(NOMBRE DEL AMPA)* para la prestación de servicios que no comportan el acceso a datos personales de ficheros o sistemas de los cuales es responsable.

Prestador	**Servicio**
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
(indicar la denominación del tercero)	*(indicar el servicio contratado)*

Anexo INF007

INF007	*Autorizacion salida de soportes*

FECHA VERSIÓN DEL ANEXO INF007	*(fecha de alta)*
VERSIÓN	*(001)*

El/la Presidente/Presidenta de la *(NOMBRE DEL AMPA)* autoriza la salida del soporte entregándolo a la persona que se hace responsable hasta su devolución, no estando permitido cederlos a terceros ni a realizar copias.

Persona .....

DNI .....

Anexo REG001

REG001	*Entrega del documento de seguridad*

FECHA VERSIÓN DEL ANEXO REG001	*(fecha de alta)*
VERSIÓN	*(001)*

Usuario	**Fecha entrega**	**Firma del receptor**
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
.....	.....	.....
(nombre de la persona)	*(fecha de alta)*	

(Añadir tantas filas como sea necesario)

Anexo REG002

REG002	*Registro de incidencias*

FECHA VERSIÓN DEL ANEXO REG002	*(fecha alta)*
VERSIÓN	*(001)*

(La información registrada de cada incidencia se incluye en una ficha separada y numerada)

Código incidencia

Número ..... *(indicar el número de la incidencia, por ejemplo 1-2016)*

Tipo o descripción del incidente	*(describir las circunstancias en que se ha producido la incidencia)*
Momento en que se ha producido	*(indicar el día, la hora y el minuto, si es posible)*
Momento en que se ha detectado	*(indicar el día, la hora y el minuto, si es posible)*
Persona que ha notificado la incidencia	*(indicar nombre y apellidos)*
Persona a quien se ha notificado la incidencia	*(indicar nombre y apellidos)*
Consecuencias de la incidencia	*(describir cómo afecta la incidencia a los datos)*
Medidas adoptadas	*(describir qué medidas correctoras se han adoptado a raíz de la incidencia)*
Restauración de datos	*(sí/no, indicar si ha sido necesario restaurar datos)*
Otras informaciones en relación con la incidencia	*(añadir otras informaciones que puedan completar el registro de la incidencia)*

Operaciones de recuperación

(Hay que incluir en este documento el registro de las recuperaciones de información de ficheros de nivel medio o alto. Para los de nivel básico, sólo cuando se graben los datos manualmente)

Usuario que ha hecho la restauración *(*1)*	Fecha *(*2)*	Tipo y observaciones *(*3)*
.....	.....	.....
.....	.....	.....
.....	.....	.....

*(*1) Nombre y apellidos.*
*(*2) dd/mm/aaaa*
*(*3) Datos restaurados; si se ha hecho manualmente; otras observaciones, como la justificación de la grabación manual, etc.*

(Añadir tantas filas como sea necesario)

Anexo REG003

REG003	*Registro de copias de seguridad*

FECHA VERSIÓN DEL ANEXO REG003	*(fecha alta)*
VERSIÓN	*(001)*

Usuario que ha realizado la copia	**Fichero**	**Fecha**
.....	.....	.....
.....	.....	.....
.....	.....	.....
(nombre y apellidos)	*(nombre fichero)*	*(dd/mm/aaaa)*

Tipo y observaciones .....

.....

.....

.....

.....

Anexo REG004

REG004	*Inventario de soportes*

FECHA VERSIÓN DEL ANEXO REG004	*(fecha alta)*
VERSIÓN	*(001)*

Inventario de los soportes tanto electrónicos como en papel, que contienen datos de carácter personal del fichero *(NOMBRE FICHERO)*.

A) SOPORTES ELECTRÓNICOS

Etiqueta del soporte	*(indicar la información que tiene que constar en la etiqueta)*
Ubicación del soporte	*(indicar el lugar donde se encuentra el soporte)*
Tipo y observaciones	*(indicar el tipo de copia y las observaciones apropiadas, por ejemplo Memoria USB - Soporte destinado a copias de seguridad)*
Personas autorizadas a acceder	*(indicar nombre y apellidos)*
Autorización de salida	*(G= General / P = Puntual)*
Instrucciones de seguridad	*(describir las instrucciones especiales para el transporte del soporte)*

B) SOPORTES EN PAPEL

Tipo de expediente o información: .....

Etiqueta del soporte	*(indicar la información que tiene que constar en la etiqueta)*
Ubicación del soporte	*(indicar el lugar donde se encuentra el soporte)*
Tipo y observaciones	*(indicar el tipo de documentación y/o las observaciones apropiadas)*
Personas autorizadas a acceder	*(indicar nombre y apellidos)*
Autorización de salida	*(G= General / P = Puntual)*
Instrucciones de seguridad	*(describir las instrucciones especiales para la conservación y el transporte del soporte)*

(Añadir tantas fichas como sea necesario, una por cada soporte que se deba inventariar)

Federación de la Comunidad de Madrid
de Asociaciones de Padres
y Madres del Alumnado
"Francisco Giner de los Ríos"

Año de realización 2018