Registro de Actividades de Tratamiento y Medidas de Seguridad

Fecha	FECHA ALTA

Documento Registro de Actividades de Tratamiento

NOMBRE AMPA

CIF

DIRECCIÓN

CORREO ELECTRÓNICO

TELÉFONO

NOBRE DEL PROYECTO

Aviso de confidencialidad

A este documento, así como al resto de documentación y de informaciones relacionadas con las medidas de seguridad del tratamiento de datos personales de los que es responsable la **[NOMBRE 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

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 AMPA**. Estas medidas sirven para el registro de actividades de tratamiento y para evitar la alteración, la pérdida o el acceso no autorizado a los datos que contienen y garantizar su disponibilidad.

➢ Registro de actividades de tratamiento.

Código documento	Descripción
AT01	Descripción de la actividad de tratamiento.
AT02	Captura de los datos.
AT03	Almacenamiento de los datos.
AT04	Uso y tratamiento de los datos
AT05	Transferencias y cesiones previstas.
AT06	Destrucción.
AT07	Encargado de tratamiento.

➢ Medidas de seguridad

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. Anexo medidas de seguridad

➢ Anexos

Código documento	Descripción
INF001	Descripción del sistema informático.
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	Registro de incidencias
REG002	Registro de copias de seguridad
REG003	Inventario de soportes

Registro de Actividades de Tratamiento

AT01	*Descipción de la actividad*

1. Actividad de tratamiento.
La **NOMRE DEL AMPA** agrupa a madres, padres, tutoras y tutores legales del alumnado matriculado en el **NOMBRE DEL CENTRO**, que voluntariamente deciden unirse para la consecución de detrminado fines y objetos.
- Asistir a madres, padres, tutores y tutoras en todo lo concerniente a la educación de sus hijas e hijos.
- Colaborar en las actividades educativas de los centros. (Inluyendo actividades extraescolares).
- Promover la participacion de las familias del alumnado en la gestión del centro.
- Asistir a madres, padres, tutoras y tutores en el ejercicio de su derecho a intervenir en el control de los centros sostenidos con fondos públicos.
- Facilitar la representación y la participación de madres, padres, tutores y tutoras en los consejos escolares de los centros.
- Cualesquiera otras que entren dentro del marco normativo.

Para todo ello hace falta recabar información de madres, padres, tutoras, tutores y alumnado de las personas que se asocien.

2. Finalidad.
La información que nos facilita con el fin de prestarles el servicio solicitado, **PONER EL MOTIVO,** ***(ejemplo, realizar tareas propias de gestion administrativa de la asociacion para mandar informacion a socios/as acerca de actividades realizadas por el 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

3. Interesados.
Las personas interesadas o los usuarios afectados son los asociados y el alumnado de las personas asociadas que estén en el **NOMBRE DEL CENTRO**, así como el personal voluntario o aquellas personas que por su relación con el **NOMBRE DEL AMPA**, tenga algún tipo de acuerdo o contrato.

4. Categoría de datos.
Los datos son considerados de carácter básico haciendo refencia a identificativos y gestión de actividades.

AT02	*Captura-recogida de los datos.*

1. Actividades del proceso.
Los datos serán recogidos a través **PONER LA FORMA DE RECABARLOS** ***(Ejemplo: de formularios o por cesión de datos de los centros que con el respectivo consentimiento)***.

2. Datos tratados.
COLECTIVOS INTERESADOS ***(Ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias)***

DATOS DE CARÁCTER IDENTIFICATIVO ***(Ejemplo: nombre. apellidos, dni, dirección, teléfono, correo electrónico, cuenta corriente...)***

3. Intervinientes.
Los datos serán recogidos por:
HACER UNA LISTA DE LAS PERSONAS QUE RECOGERÁN LOS DATOS.

4. Tecnologías.
Los datos serán recogidos a traves de ***(Ejemplo: página web www.nombrepagina.com , correo electrónico, redes sociales, fax, etc.)***

AT03	*Almacenamiento de los datos.*

1. Actividades del proceso.
Los datos serán almacenados en **PONER DISPOSITIVOS DONDE SERÁN GUARDADOS** ***(Ejemplo: Pc.'s, discos duros, pendrive, dvd, cd, etc. También especificar si serán guardados en papel en armario, caja se seguridd, etc).***

2. Datos tratados.
Los datos que serán almacenados son:
COLECTIVOS INTERESADOS ***(Ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias)***

DATOS DE CARÁCTER IDENTIFICATIVO ***(Ejemplo: nombre. apellidos, dni, dirección, teléfono, correo electrónico, cuenta corriente...)***

3. Intervinientes.
Los datos serán trabajados para su almacenamiento por:
HACER UNA LISTA DE LAS PERSONAS QUE TRABAJARÁN EN EL ALMACENAMIENTO DE LOS DATOS.

4. Tecnologías.
Los datos serán almacenados a traves de ***(Ejemplo: programa informático, nube, BBDD, etc.)***

AT04	*Uso y tratamiento de los datos.*

1. Actividades del proceso.
La información suministrada será usada para..... ***(ejemplo, realizar tareas propias de gestion administrativa de la asociacion para mandar informacion a socios/as acerca de actividades realizadas por el ampa. pagos y cobros).***

2. Datos tratados.
Los datos tratados son:
COLECTIVOS INTERESADOS ***(Ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias)***

DATOS DE CARÁCTER IDENTIFICATIVO ***(Ejemplo: nombre. apellidos, dni, dirección, teléfono, correo electrónico, cuenta corriente...)***

3. Intervinientes.
Los datos serán tratados por:
HACER UNA LISTA DE LAS PERSONAS QUE TRABAJARÁN EN EL TRATAMIENTO DE LOS DATOS.

4. Tecnologías.
Los datos serán tratados a traves de ***(Ejemplo: programa informático, nube, BBDD, etc.)***

AT05	*Transferencias y cesiones previstas.*

1. Actividades del proceso.
La información podrá ser cedida a la **Consejería de eduación, centro educativo, servicios sociales o sanitarios, jueces, tribunales, cuerpos y fuerzas de seguridad del estado** y aquellos organismos que la ley así lo estipule.
Además cuando así sea solicitado por por un tercero y sea autorizado por el afectado o interesado

2. Datos tratados.
Los datos que serán transferidos o cedidos son:
Aquellos que **NOMBRE DEL AMPA** disponga previa autorización u obligación..

3. Intervinientes.
Los datos serán transferidos o cedidos por:
HACER UNA LISTA DE LAS PERSONAS AUTORIZADAS A CEDIR O TRANSFERIR.

4. Tecnologías.
Los datos podrán ser cedidos o transferidos por los medios que determine la ley o aquellos que autorice el afectado o interesado.

AT06	*Destrucción.*

1. Actividades del proceso.
Cuando por motivo de baja o se cumplan los tiempos estabecidos, la información deberá darse de baja, para lo cual se borraraán los datos que no sean obligatorios conservar o se bloquearán para que no se pueda acceder a ellos. Del mismo modo se realizará con la documentación en papel, debiendo dejar un documento que acredite la labor realizada.

2. Datos tratados.
Los datos que serán destruidos son:
Aquellos que **NOMBRE DEL AMPA** disponga y no sean relevantes o la ley obligue a conservar.

3. Intervinientes.
Los datos serán destruidos por:
HACER UNA LISTA DE LAS PERSONAS AUTORIZADAS A DESTRUIR LOS DATOS.

4. Tecnologías.
Los datos serán destruidos de forma que no puedan ser usados. Para ellos se se establecerá el programa informátco adecado, ***(ejemplo eraser),*** y en papel a través de destructora.

AT07	*Encargado de tratamiento.*

1. Encargado de tratamiento.

DATOS IDENTIFICATIVOS DEL ENCARGADO DE TRATAMIENTO: NOMBRE DNI/CIF, DIRECCIÓN,ETC

2. Categorías de tratamiento.
Los datos serán tratados son de tipo identificativo. **PONER LOS DATOS QUE SE HAN PASADO**

COLECTIVOS INTERESADOS ***(Ejemplo: alumnado, padres, madres, tutores, tutoras, monitores, monitoras, personas voluntarias)***

DATOS DE CARÁCTER IDENTIFICATIVO ***(Ejemplo: nombre. apellidos, dni, dirección, teléfono, correo electrónico, cuenta corriente...)***

Documento Registro de Medidas de Seguridad (Suple al Análisis de Riesgo)

NOMBRE AMPA

CIF

DIRECCIÓN

CORREO ELECTRÓNICO

TELÉFONO

NOBRE DEL PROYECTO

1.Ámbito de alicación del documento.

Este documento de Registro de actividades contiene además las medidas de seguridad del que es reponsable **NOMBRE DEL AMPA.**

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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,

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

3. Funciones y obligaciones de las personas autorizadas a tratar los datos

Las personas que tengan acceso o que traten los datos contenidos en los ficheros de la **NOMBRE AMPA** tienen que conocer y observar las medidas de seguridad y obligaciones relacionadas establecidas en este 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 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 personal ajeno a la **NOMBRE 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 medidas 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 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 documento 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 puedan acceder a la información, hay que contar con la autorización del responsable del fichero.

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 AMPA**, dar de alta y de baja a los usuarios al sistema y proporcionarles el código de usuario y la palabra de paso asignada que se dará directaente en sobre cerrado. La palabra de paso 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 paso o contraseña cada seis meses.

3.3. Responsable de medidas de seguridad

Se designa como responsable de medidas de seguridad a **el/la Presidente/Presidenta de la NOMBRE AMPA**, que se encarga de coordinar y controlar las medidas establecidas en este documento.

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

El responsable de medidas 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 AMPA**, requiere la suscripción del contrato o el acuerdo de encargo y se considera un encargado de tratamiento.

En el documento anexo **INF005**, se relacionan los terceros que actúan como encargados del tratamiento por cuenta de la **NOMBRE AMPA**, con indicación de si los datos necesarios para prestar los servicios se tratan en los locales de la **NOMBRE 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 AMPA**.*

Si, de conformidad con el contrato o el acuerdo de encargo suscrito, el servicio se presta en los locales de la **NOMBRE 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 AMPA**,

El personal del encargado del tratamiento tiene que cumplir las medidas de seguridad previstas en este documento de modelo 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.

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

Para que los datos se puedan tratar fuera de los locales de la **NOMBRE AMPA**, así como para incorporarlos en dispositivos portátiles, hace falta que la autorización conste en el Anexo **INF002**. 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 medidas seguridad.

Si se ha establecido que el encargado tiene que devolver, al responsable de los ficheros o a otro encargado que 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 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 modelo de seguridad y, en cualquier caso, se tiene que certificar por escrito. Este certificado se tiene que transmitir a la **NOMBRE 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 modelo de seguridad.

El encargado del tratamiento tiene que poner en conocimiento de **el/la Presidente/Presidenta de la NOMBRE 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 modelo 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 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 Registro de Actividades de Tratamiento.

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 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 medidas 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 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 medidas 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 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 medidas de seguridad. Todo esto, sin perjuicio 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 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 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 AMPA**, sin acceso a datos personales.

El acceso a los lugares en que están ubicados los servidores de la **NOMBRE AMPA**, se tiene que hacer cuando esté presente personal de la **NOMBRE 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 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 AMPA, de conformidad con el procedimiento establecido en el apartado 5 de este documento de modelo 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 además de estar registradas en el Registro de Actividades de Tratamiento.

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 documentos **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 fitcheros 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 LOPD y lo que establece este documento de modelo 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 AMPA**

Se pueden hacer los tratamientos de datos personales de los ficheros, fuera de los locales de la **NOMBRE 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 modelo de seguridad, así como cualquier otra anomalía que afecta o pueda afectar a la seguridad de los datos personales de la **NOMBRE AMPA**.

Las personas relacionadas en el anexo **INF002** tienen que comunicar lo antes posible la incidencia a **el/la Presidente/Presidenta de la NOMBRE 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 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 AMPA tiene que anotar en el registro de incidencias, (ver documento anexo **REG001**), 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 en todo 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 AMPA**.

Cada seis meses **el/la Presidente/Presidenta de la NOMBRE 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 modelo de seguridad.

En el documento **REG002** 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 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 **REG003** 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 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 **NOMBRE FICHERO_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 seguridas previstas en el RGPD y LOPD.

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 la tiene que custodiar 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 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 modelo 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 de la forma siguiente **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 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

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 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.

2. . Información en soporte papel

Se pueden destruir documentos en soporte papel que incluyan datos personales, de acuerdo con el sistema siguiente:

Utilizar la destructora de papel ubicada en la **NOMBRE AMPA**.

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

9. Auditoría

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

10. Anexo medias 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 personales 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) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), 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 mínimas 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 datos personales y serán informados acerca de dichas 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 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 (VIDEOVIGILANCIA)

    - **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 mediante 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 el 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 media 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 para 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 pueden ser de utilidad para su empresa o su actividad profesional.

Anexo INF001

INF001	*Sistemas informatícos*

Equipos informáticos con los cuales se tratan los datos del fichero

HARDWARE

Marca y modelo del ordenador:
Número de serie:

Anexo INF002

INF002	*Usuarios y autorizaciones de acceso a los datos*

Relación de usuarios autorizados a: RECOGIDA DE DATOS.

Usuario	NOMBRE PERSONA	FIRMA
Cargo / función	PRESIDENTE/A	
Otros puertos / interfaces externas	REMOTO/NUBE/CORREO/WEB	

Relación de usuarios autorizados al: ALMACENAMIENMTO DE DATOS.

Usuario	NOMBRE PERSONA	FIRMA
Cargo / función	PRESIDENTE/A	
Otros puertos / interfaces externas	REMOTO/NUBE/CORREO/WEB	

Relación de usuarios autorizados al: TRATAMIENTO DE DATOS.

Usuario	NOMBRE PERSONA	FIRMA
Cargo / función	PRESIDENTE/A	
Otros puertos / interfaces externas	REMOTO/NUBE/CORREO/WEB	

Relación de usuarios autorizados al: TRANSFERENCIAS Y CESIONES DE DATOS.

Usuario	NOMBRE PERSONA	FIRMA
Cargo / función	PRESIDENTE/A	
Otros puertos / interfaces externas	REMOTO/NUBE/CORREO/WEB	

Relación de usuarios autorizados al: DESTRUCCIÓN DE DATOS.

Usuario	NOMBRE PERSONA	FIRMA
Cargo / función	PRESIDENTE/A	
Otros puertos / interfaces externas	REMOTO/NUBE/CORREO/WEB	

Anexo INF003

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

Identificación del fichero: NOMBRE FICHERO
Sistema de tratamiento: MIXTO

Datos de: COLECTIVOS INTERESADOS : DATOS DE CARACTER IDENTIFICATIVO

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

(Datos de carácter identificativo hace refeencia 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*

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

Usuario autorizado Nombre y Apellidos	**Tipo de Autorización ***	**Fecha autorización**	**Firma**	**Fecha revocación**	**Firma**

**Tipo de Autorización:*
Trat_DD: Tratamiento/Modificación de Datos en soporte y/o BBDD
Dest_DD: Destrucción de Datos/Soporte
BKP_DD: Copia de Seguridad Datos
Salida_DD: Salida/Traslado de dispositivos/soportes portátiles
Inventario: Inventariar / Etiquetar soportes y copias de seguridad.
Otros: Especificar y numerar en observaciones. Incluir fecha.

Otras autorizaciones no especificadas:

Otro tipo de Autorización	**Fecha**

Anexo INF005

INF005	*Encargados del tratamiento*

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)*.
Datos tratados *(Nombre, apellidos, DNI, tfno., dirección, correo….)*

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 y LOPD 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.
- ✓ Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

  1. Acceso, rectificación, supresión y oposición
  2. Limitación del tratamiento
  3. Portabilidad de datos
  4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

  Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección …… (dirección que indique el responsable). La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

✓ Derecho de información

(Escoger una de las opciones)
Opción A El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.
Opción B Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos

✓ 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 y el número aproximado de interesados afectados, y las categorías 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 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 realicen 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 y LOPD por parte del encargado.

c) Supervisar el tratamiento.

Fecha

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

Anexo INF006

INF006	*Prestadores de servicios sin acceso a datos*

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

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

Anexo INF007

INF007	*Autorizacion salida de soportes*

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

Usuario autorizado Nombre y Apellidos/DNI	**Soporte**	**Fecha salida**	**Firma**	**Fecha devolución**	**Firma**

.....

Anexo REG001

REG001	*Registro de incidencias*

(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 1-2019)*

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	Fecha	Tipo y observaciones
Nombre y apellidos	dd/mm/aaaa	*(datos restaurados; si se ha hecho manualmente; otras observaciones, como la justificación de la grabación manual).*
Nombre y apellidos	dd/mm/aaaa	

(Añadir tantas filas como sea necesario)

Anexo REG002

REG002	*Registro de copias de seguridad*

Usuario que ha realizado la copia	**Fichero**	**Fecha**
Nombre y apellidos	**NOMBRE FICHERO**	dd/mm/aaaa

Tipo y observaciones .....

Anexo REG003

REG003	*Inventario de soportes*

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:	*Ver anexo INF002*
Autorización de salida:	*(G= General / P = Puntual*)
Instrucciones de seguridad:	*(describir las instrucciones especiales para el transporte del soporte, ejemplo bloqueo contraseña)*

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:	*Ver anexo INF002*
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)