REGISTRO DE ACTIVIDAD DEL TRATAMIENTO

ASOCIACIÓN BASIDA

REGISTRO DE ACTIVIDAD DEL TRATAMIENTO

ÍNDICE

1. OBJETO DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El presente documento (Registro de Actividades de Tratamiento, en adelante RAT), tiene por objeto dar cumplimiento a lo establecido en el Art. 30 del Reglamento Europeo de Protección de Datos UE 679/2016, de 27 de Abril, del Parlamento y el Consejo (RGPD), en el art. 31 de la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), y en el resto de la normativa nacional vigente, y para ello se realizan las siguientes operaciones:

1º.- Realizar una identificación completa del Responsable del Tratamiento y, en su caso, del Corresponsable, del Representante del Responsable (en caso de que el Responsable del Tratamiento no tuviera su establecimiento en España), y del Delegado de Protección de Datos, señalando los datos de contacto de los mismos.

2º.- Realizar una descripción de las categorías de interesados y de las categorías de datos personales que se hayan incluidos y tratados en el sistema de tratamiento de datos de la entidad ASOCIACIÓN BASIDA como Responsable del Tratamiento.

3º.- Realizar una descripción de las finalidades de los distintos tratamientos de datos.

4º.- Realizar una descripción de las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

5º.- Realizar una descripción de las comunicaciones de datos a terceros, cuando estos actúen en calidad de Encargados de Tratamiento o Cesionarios, si los hubiere.

6º.- Realizar una descripción, en el caso de producirse una transferencia internacional de datos a un tercer país u organización internacional; de los destinatarios, de los datos transferidos, del tercer país u organización internacional de que se trate y de la justificación de las garantías adecuadas.

7º.- Cuando sea posible, determinar los plazos previstos para la supresión de las diferentes categorías de datos.

8º.- Cuando sea posible, realizar una descripción general de las medidas técnicas y organizativas de seguridad establecidas en el art. 32, apartado 1 del RGPD (la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento). Contemplado en el art. 28.1 de la LOPDGDD.

ELEMENTO ADICIONAL

Mediante la realización de una Evaluación de Riesgos y, en su caso, de Impacto, se analizarán los posibles riesgos inherentes al Tratamiento llevado a cabo por el Responsable.

En el caso de la Evaluación de Impacto adicionalmente se determinará el daño que se puede producir para la confidencialidad, integridad y seguridad de los datos que dicho Responsable ha de garantizar. Como conclusión, en esta Evaluación de Impacto (EIPD), se establecerán las medidas que se recomiendan adoptar para evitar o minimizar riesgos y daños (art. 35 del RGPD y art. 28.1 de la LOPDGDD).

2. RESPONSABLE DEL TRATAMIENTO

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO Y DATOS DE CONTACTO, CORRESPONSABLE, REPRESENTANTE Y DELEGADO DE PROTECCIÓN DE DATOS (SI EXISTEN).

Responsable del Tratamiento

Razón Social:	ASOCIACIÓN BASIDA
CIF NIF :	G79186466
Dirección :	CARRETERA ANTIGUA DE TOLEDO, KM. 9
Código Postal:	28300
Localidad:	ARANJUEZ
Provincia:	MADRID
Teléfono:	918923537
Email:	aranjuez@basida.org
WEB:	https://basida.com/

Nombre y Apellidos del Representante	VISITACIÓN ADÁN VILLAREAL
NIF del Representante Legal:	07480655C
Cargo del Representante Legal:	PRESIDENTA

Delegado Protección de Datos

Razón Social:	GRUPO DATA CUMPLIMIENTO NORMATIVO S.L.
CIF NIF :	B10367654
Dirección :	CL. PERIODISTA SANCHEZ ASENSIO Nº 5
Código Postal:	10002
Localidad:	CACERES
Provincia:	CÁCERES
Teléfono:	927600000
Email:	dpo@grupodata.es

3. IDENTIFICACIÓN Y DESCRIPCIÓN DE TRATAMIENTOS

Se han identificado como Tratamiento todas aquellas operaciones que se realizan, automatizadas o no, y finalidades de dichas operaciones, teniendo en cuenta los distintos colectivos de titulares de datos de carácter personal con los que se relaciona el Responsable del Tratamiento.

Tratamiento: **RESIDENTES**

Sistema: MIXTO Nivel de Seguridad : ALTO Tipo: PRIVADO

Descripción de la Finalidad: RESIDENTES

Otras Finalidades: GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA, GESTIÓN DE ASOCIADOS O MIEMBROS DE PARTIDOS POLITICOS, SINDICATOS, IGLESIAS, CON, OTRAS FINALIDADES.

Colectivos:

CARACTERÍSTICAS Y TIPOLOGÍA DE LOS DATOS DEL TRATAMIENTO RESIDENTES

Origen: El propio interesado o su representante legal. Otras personas físicas. Registros públicos. Entidad privada. Administraciones Públicas.

Especialmente Protegidos: Salud.

Identificativos: NIF. Nº SS / Mutualidad. Nombre y Apellidos. Dirección. Firma Manual (Manuscrita o Digitalizada). Teléfono. Imagen / Voz.

Caracteristicas Personales: Datos de Características Personales.

Academicos Profesionales: Datos Académicos y Profesionales.

Detalles de Empleo: Datos de Detalles de Empleo.

Economico Financieros y Seguros: Datos Económicos - Financieros - Seguros.

Transacciones: Datos de Transacciones.

Tratamiento: **SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES**

Sistema: MIXTO Nivel de Seguridad : BÁSICO Tipo: PRIVADO

Descripción de la Finalidad: GESTIÓN INTEGRAL DE LAS RELACIONES CON LOS PROVEEDORES DE LA ENTIDAD.

Otras Finalidades: GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA.

Colectivos: PROVEEDORES.

CARACTERÍSTICAS Y TIPOLOGÍA DE LOS DATOS DEL TRATAMIENTO SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES

Origen: El propio interesado o su representante legal.

Identificativos: NIF. Nombre y Apellidos. Dirección. Firma Manual (Manuscrita o Digitalizada). Teléfono.

Tratamiento: **VOLUNTARIOS**

Sistema: MIXTO Nivel de Seguridad : BÁSICO Tipo: PRIVADO

Descripción de la Finalidad: VOLUNTARIOS

Otras Finalidades: GESTIÓN CONTABLE, FISCAL Y ADMINISTRATIVA, OTRAS FINALIDADES, PUBLICIDAD Y PROSPECCIÓN COMERCIAL.

Colectivos:

CARACTERÍSTICAS Y TIPOLOGÍA DE LOS DATOS DEL TRATAMIENTO VOLUNTARIOS

Origen: El propio interesado o su representante legal.

Identificativos: NIF. Nombre y Apellidos. Dirección. Firma Manual (Manuscrita o Digitalizada). Teléfono. Imagen / Voz.

Tratamiento: **VIDEOVIGILANCIA**

Sistema: AUTOMÁTICO Nivel de Seguridad : BÁSICO Tipo: PRIVADO

Descripción de la Finalidad: SEGURIDAD Y CONTROL EN LAS INSTALACIONES DE LA ENTIDAD

Otras Finalidades: VIDEOVIGILANCIA.

Colectivos: CLIENTES Y USUARIOS, EMPLEADOS, PROVEEDORES, PÚBLICO EN GENERAL.

CARACTERÍSTICAS Y TIPOLOGÍA DE LOS DATOS DEL TRATAMIENTO VIDEOVIGILANCIA

Origen: El propio interesado o su representante legal.

Identificativos: Imagen / Voz.

Cesiones Publicas: Fuerzas y Cuerpos de Seguridad.

DATOS COMUNES A TODOS LOS TRATAMIENTOS

Equipos Informáticos:

Total Equipos: 14

Tipo Equipo	Descripción	Númer	Contraseña	Remoto	SistemaOperativo
EQUIPO SOBREMESA	ORDENADOR	13	☑	☐	MICROSOFT WINDOWS 95/98/2000/XP/VISTA/ 7/8/10
SERVIDOR	SERVIDOR	1	☑	☐	WINDOWS SERVER

Aplicaciones Informáticas:

Tipo de Aplicación	Descripción Aplicación Informática	Observaciones
ANTIVIRUS	ANTIVIRUS	
SUITE OFIMÁTICA	OFFICE	

Copias de Seguridad:

Procedimiento:	COPIA EN DISCO DURO EXTERNO
Lugar de Almacenamiento:	
Frecuencia:	SEMANALMENTE
Dispositivo de Copia:	DISCO DURO EXTERNO
Servicio:	INTERNO
Otra Frecuencia:	
Responsable Copia:	CRISTINA ALONSO BURGO

Sedes y Tratamientos Contenidos:

Sede: ***BASIDA-ARANJUEZ***

Dirección : CARRETERA ANTIGUA DE TOLEDO, KM. 9

C. Postal : 28300

Población : ARANJUEZ

Provincia : MADRID

Región : COMUNIDAD DE MADRID

Pais : ESPAÑA

Tratamientos en Sede:

RESIDENTES, SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES, VIDEOVIGILANCIA, VOLUNTARIOS

Sede: ***BASIDA-MANZANARES***

Dirección : CARRETERA CIUDAD REAL N. 430, KM. 361

C. Postal : 13200

Población : MANZANARES

Provincia : CIUDAD REAL

Región : CASTILLA LA MANCHA

Pais : ESPAÑA

Tratamientos en Sede:

RESIDENTES, SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES, VOLUNTARIOS

Sede:	***BASIDA-NAVAHONDILLA***
Dirección :	AV. RESIDENCIA SANTA ISABEL Nº 17
C. Postal :	05429
Población :	NAVAHONDILLA
Provincia :	AVILA
Región :	CASTILLA LEON
Pais :	ESPAÑA

Tratamientos en Sede:

RESIDENTES, SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES, VOLUNTARIOS

Medidas de protección de los locales donde están ubicados los Tratamientos

Como medidas de seguridad para la protección del centro de tratamiento donde están ubicados los tratamientos con datos de carácter personal, la entidad **ASOCIACIÓN BASIDA** ha optado por utilizar:

Medidas de Seguridad:

BASIDA-ARANJUEZ

Cámaras de Videovigilancia :	☐
Carteles Informativos Visibles :	☐
Logos y Contactos :	☐
Alarma :	☐
Grabaciones :	☐
Extintores :	☑
Detectores de humo :	☐
Puertas de seguridad :	☑
Vigilante de Seguridad :	☐
Portero automático :	☐
Sitios Acceso Restringido	ACCESO RESTRINGIDO
Envios Telemáticos :	
Comunicaciones :	
Observaciones :	

BASIDA-MANZANARES

Cámaras de Videovigilancia :	☐
Carteles Informativos Visibles :	☐
Logos y Contactos :	☐
Alarma :	☐
Grabaciones :	☐
Extintores :	☑
Detectores de humo :	☐
Puertas de seguridad :	☑
Vigilante de Seguridad :	☐
Portero automático :	☐
Sitios Acceso Restringido	ACCESO RESTRINGIDO
Envios Telemáticos :	
Comunicaciones :	
Observaciones :	

BASIDA-NAVAHONDILLA

Cámaras de Videovigilancia :	☐
Carteles Informativos Visibles :	☐
Logos y Contactos :	☐
Alarma :	☐
Grabaciones :	☐
Extintores :	☑
Detectores de humo :	☐
Puertas de seguridad :	☑
Vigilante de Seguridad :	☐
Portero automático :	☐
Sitios Acceso Restringido	ACCESO RESTRINGIDO
Envios Telemáticos :	
Comunicaciones :	
Observaciones :	

Usuarios:

MARIA LUISA MARTOS GARCIA	-	07479922T	-	GUARDIA DE NOCHE	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Juan Carlos Becerra González	-	29777547E	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Arancha Lloret Sáez-Bravo	-	07479132S	-	RESPONSABLE SANITARIO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Félix Mendívil Ochoa	-	72665716E	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Elena Colastra Sansegundo	-	02705740C	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Pedro Izquierdo Peñaranda	-	70040190S	-	RESPONSABLE JURIDICO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Pedro Izquierdo Peñaranda	-	70040190S	-	RESPONSABLE JURIDICO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Pedro Izquierdo Peñaranda	-	70040190S	-	RESPONSABLE JURIDICO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Josefa de la Varga Domínguez	-	06735476H	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Asunción La Moneda González	-	51440623L	-	RESPONSABLE CALIDAD	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Asunción La Moneda González	-	51440623L	-	RESPONSABLE CALIDAD	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Asunción La Moneda González	-	51440623L	-	RESPONSABLE CALIDAD	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Cristina Alonso Burgo	-	07480103C	-	RESPONSABLE PROTECCIÓN DE DATOS	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Cristina Alonso Burgo	-	07480103C	-	RESPONSABLE PROTECCIÓN DE DATOS	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Cristina Alonso Burgo	-	07480103C	-	RESPONSABLE PROTECCIÓN DE DATOS	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Jorge Ruiz Escagedo	-	07485941Q	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Jorge Ruiz Escagedo	-	07485941Q	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Jorge Ruiz Escagedo	-	07485941Q	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Jokin Uribarren Zapiraín	-	30581085D	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Jokin Uribarren Zapiraín	-	30581085D	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS

Jokin Uribarren Zapiraín	-	30581085D	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
ALBA GÁMEZ MANSO	-	50337941A	-	ALUMNO/A EN PRÁCTICAS	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Alfonso Octavio Moreno Merino	-	09030006E	-	PSICOLOGO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
VISITACIÓN ADÁN VILLAREAL	-	07480655C	-	DIRECTORA	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
VISITACIÓN ADÁN VILLAREAL	-	07480655C	-	DIRECTORA	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
VISITACIÓN ADÁN VILLAREAL	-	07480655C	-	DIRECTORA	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Francisca Rosado Bas	-	08782960L	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
María del Carmen Rodriguez de Guzmán Romero	-	70029155C	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Teresa Fernández Seguro	-	50488355C	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Ignacio Ruíz Fernández	-	13560876F	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Dolores Planas Comerma	-	39133570J	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Rosario Adán Villarreal	-	07480652V	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Mario Núñez Alcázar de Velasco	-	03223807N	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Raúl Murillo Gallego	-	70044898P	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Javier Marqués Martinez	-	70033355B	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Darmín Belmar Buendía	-	04591890D	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Laura Tainio	-	Y1428409P	-	RESPONSABLE SANITARIO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Dolores García-Núñez Patón	-	70737534E	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Blanca Noblejas Solís	-	52382101S	-	PSICÓLOGA	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
María Antonia Romero de Ávila	-	70737603E	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
León Trujillo García	-	02061229S	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Paloma Adán Villarreal	-	07485477N	-	DIRECTORA	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS

Rafael Lorenzo-Arroyo Poullet	-	05402742L	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Elena Rodelgo Rincón	-	46840316B	-	RESPONSABLE SANITARIO	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
María Soledad Matarranz Carreras	-	03417764X	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Ángel Javier Miranda Estibaliz	-	16036197E	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Cristina Sánchez del Hoyo	-	12421819W	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Miguel Martín Asenjo	-	72892271G	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Amaya Domínguez López de Castro	-	52993810Q	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Pablo González de la Torre	-	50310703C	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Rocío Lloret Chao	-	53767532H	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Rocío Lloret Chao	-	53767532H	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Inmaculada Ruiz Fincias	-	45687167J	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Inmaculada Ruiz Fincias	-	45687167J	-	SANITARIO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Iván Mejías Pérez	-	05284250T	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS
Iván Mejías Pérez	-	05284250T	-	ADMINISTRATIVO/A	-	NO TRABAJADOR CON ACCESO A TODOS LOS SISTEMAS

4. IDENTIFICACIÓN DE LOS ENCARGADOS DEL TRATAMIENTO

Encargado del Tratamiento

Razón Social:	ENSO AUDIT & CONSULTING S.L.
CIF / NIF:	B72761984
Dirección:	C/. MARQUES DE URQUIJO Nº 32
Localidad:	MADRID
Código Postal:	28008
Provincia:	MADRID
Nombre y Apellidos del Representante Legal:	
NIF del Representante Legal:	
Cargo del Representante Legal:	

Tratamiento	Servicio Encargado
SOCIOS, EMPRESAS COLABORADORAS Y	AUDITORIA CONTABLE

Encargado del Tratamiento

Razón Social:	GRUPO DATA CUMPLIMIENTO NORMATIVO S.L.
CIF / NIF:	B10367654
Dirección:	CL. PERIODISTA SANCHEZ ASENSIO Nº 5
Localidad:	CACERES
Código Postal:	10002
Provincia:	CÁCERES
Nombre y Apellidos del Representante Legal:	MANUEL GRANADO SANCHEZ
NIF del Representante Legal:	44406084F
Cargo del Representante Legal:	DIRECTOR GENERAL

Tratamiento	Servicio Encargado
SOCIOS, EMPRESAS COLABORADORAS Y	ASESORAMIENTO Y/O CONSULTORIA EN PROTECCIÓN DE DATOS
VOLUNTARIOS	ASESORAMIENTO Y/O CONSULTORIA EN PROTECCIÓN DE DATOS

5. ENCARGOS DEL TRATAMIENTO AL RESPONSABLE DEL TRATAMIENTO

RAZON SOCIAL RT	NIF/CIF RT	FINALIDAD	TRATAMIENTO	TID/PAIS *	NIVEL

* Transferencias Internacionales de Datos

6. IDENTIFICACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Se identificarán aquellos Tratamientos en los que existan Transferencias de Datos a Terceros Países u Organizaciones Internacionales.

EL Responsable del Tratamiento no realiza transferencias internacionales de datos en el desarrollo de su actividad, para este Tratamiento.

Tratamiento : **RESIDENTES**

EL Responsable del Tratamiento no realiza transferencias internacionales de datos en el desarrollo de su actividad, para este Tratamiento.

Tratamiento : **SOCIOS, EMPRESAS COLABORADORAS Y PROVEEDORES**

EL Responsable del Tratamiento no realiza transferencias internacionales de datos en el desarrollo de su actividad, para este Tratamiento.

Tratamiento : **VOLUNTARIOS**

EL Responsable del Tratamiento no realiza transferencias internacionales de datos en el desarrollo de su actividad, para este Tratamiento.

Tratamiento : **VIDEOVIGILANCIA**

7. DETERMINACIÓN DE LAS MEDIDAS DE SEGURIDAD A APLICAR TRAS EL INICIAL ANÁLISIS DE RIESGOS DE PROTECCIÓN DE DATOS

De acuerdo con lo estipulado en el art. 35 del RGPD, y en el art. 28.1 de la LOPDGDD, será imprescindible realizar una Evaluación de Impacto cuando concurran algunas de las siguientes circunstancias:

1.- Que el tratamiento de datos tenga por objeto la Elaboración de Perfiles y Análisis Automatizado de Aspectos Personales.

2.- Que se trate de un tratamiento a gran escala de categorías especiales de datos personales.

3.- Que el objetivo sea una observación sistemática a gran escala de zonas de acceso público.

Independientemente de que exista la obligación legal o no de realizar un Evaluación de Impacto, y en aplicación del principio de Responsabilidad Proactiva que le incumbe al Responsable, se han determinado las medidas técnico-organizativas que se consideran necesarias adoptar, tras el inicial análisis de riesgos realizado, con el objetivo de eliminar o minimizar dichos riesgos que entraña el Tratamiento de Datos de Carácter Personal para la seguridad de la información (integridad, confidencialidad-privacidad y disponibilidad de los mismos).

Se han determinado dos niveles de medidas a aplicar a cada uno de los Tratamientos incluidos en este Registro. Se les ha denominado Básico y Alto.

Los criterios principales que se han tenido en cuenta, para determinar el nivel que le corresponde a cada Tratamiento, han sido, entre otros:

a) Si se trata de datos englobados en los denominados Datos de Categoría Especial.

b) Si el tratamiento de datos lo lleva a cabo más de una persona.

c) Si hay cesiones o comunicaciones de datos a terceros.

d) Necesidad de realizar una EIPD.

e) En general, el art. 32 del RGPD y la LOPDGDD establecen: 'Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el Responsable y el Encargado del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo'.

MEDIDAS DE SEGURIDAD A APLICAR EN TRATAMIENTOS DE NIVEL BASICO	
Tratamientos Automatizados	
Funciones y obligaciones de los usuarios	- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el Registro de Actividades de Tratamiento. - Definir las funciones de control o autorizaciones delegadas por el Responsable del Tratamiento. - Formación e información de los usuarios para que conozcan de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
Usuarios y control de accesos	- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones. - Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. - Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. - Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el Registro de Actividades de Tratamiento, conforme a los criterios establecidos por el Responsable del Tratamiento. - El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
Identificación y autenticación	- Adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. - Establecer mecanismos para la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. - Si se usan contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. - El Registro de Actividades de Tratamiento establecerá un cambio periódico de contraseñas nunca superior a un año. Mientras estén vigentes, se almacenarán de forma ininteligible.
Registro de Incidencias	- Establecer un procedimiento de notificación y gestión de las incidencias. - Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Gestión de soportes y documentos	Etiquetado	- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. - No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. - Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.
	Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del Responsable del Tratamiento deberá ser autorizada por el Responsable del Tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.
	Traslado	En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
	Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
Copias de respaldo y recuperación	Copia de respaldo	- Copia como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. - Fijar procedimientos para la recuperación de los datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. - En tratamientos parcialmente automatizados si existe documentación que permite la reconstrucción se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Registro de Actividades de Tratamiento.
	Control periódico	Control periódico semestral de la definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
	Pruebas con datos reales	Prohibición de pruebas con datos reales anteriores a la implantación o modificación de los sistemas de información salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el Registro de Actividades de Tratamiento. Deberá haberse realizado una copia de seguridad.
Identificación y autenticación	El Responsable del Tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.	

Control de acceso físico	Exclusivamente el personal autorizado en el Registro de Actividades de Tratamiento podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
Registro de incidencias: recuperación de datos	- El registro deberán consignar además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. - Será necesaria la autorización del Responsable del Tratamiento para la ejecución de los procedimientos de recuperación de los datos.
Controles Periódicos de Verificación	La veracidad de los datos contenidos en el Registro de Actividades de Tratamiento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías que supongan un riesgo en el cumplimiento de la Ley Orgánica de Protección de Datos Personales.
Tratamientos No Automatizados	
Funciones y obligaciones de los usuarios	- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el Registro de Actividades de Tratamiento. - Definir las funciones de control o autorizaciones delegadas por el Responsable del Tratamiento. - Formación e información del personal para que conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento
Usuarios y control de accesos	- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones. - Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. - Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. - Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el Registro de Actividades de Tratamiento, conforme a los criterios establecidos por el Responsable del Tratamiento. - El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
Registro de incidencias	- Establecer un procedimiento de notificación y gestión de las incidencias - Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas

Gestión de soportes y documentos	Etiquetado	- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. - No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. - Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.
	Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del Responsable del Tratamiento deberá ser autorizada por el Responsable del Tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.
	Traslado	En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
	Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
	Custodia de los soportes	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el Responsable del Tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.
	Dispositivos de almacenamiento	Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.
Criterios de archivo	El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el Responsable del Tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.	

Controles Periódicos de Verificación	La veracidad de los datos contenidos en el Registro de Actividades de Tratamiento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías que supongan un riesgo en el cumplimiento de la Ley Orgánica de Protección de Datos Personales.
MEDIDAS DE SEGURIDAD A APLICAR EN TRATAMIENTOS DE NIVEL ALTO	
Tratamientos Automatizados	
Funciones y obligaciones del personal	- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el Registro de Actividades de Tratamiento. - Definir las funciones de control o autorizaciones delegadas por el Responsable del Tratamiento. - Formación e información del personal para que conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
Usuarios y control de accesos	- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones. - Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. - Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. - Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el Registro de Actividades de Tratamiento, conforme a los criterios establecidos por el Responsable del Tratamiento. - El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
Identificación y autenticación	- Adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios. - Establecer mecanismos para la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. - Si se usan contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. - El Registro de Actividades de Tratamiento establecerá un cambio periódico de contraseñas nunca superior a un año. Mientras estén vigentes, se almacenarán de forma ininteligible.

Registro de Incidencias	- Establecer un procedimiento de notificación y gestión de las incidencias. - Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.	
Gestión de soportes y documentos	Etiquetado	- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. - No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. - Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.
	Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del Responsable del Tratamiento o tratamiento deberá ser autorizada por el Responsable del Tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.
	Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
Copias de respaldo y recuperación	Copia de respaldo	- Copia como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. - Fijar procedimientos para la recuperación de los datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. - En tratamientos parcialmente automatizados si existe documentación que permite la reconstrucción se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el Registro de Actividades de Tratamiento.
	Control periódico	Control periódico semestral de la definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

	Pruebas con datos reales	Prohibición de pruebas con datos reales anteriores a la implantación o modificación de los sistemas de información salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el Registro de Actividades de Tratamiento. Deberá haberse realizado una copia de seguridad.
Responsable de Seguridad	Designación	En el Registro de Actividades de Tratamiento deberán designarse uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en el mismo.
	Tipos de designación	- Única para todos los tratamientos de datos de carácter personal. - Diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el Registro de Actividades de Tratamiento.
Auditoría	Periodicidad	Al menos cada dos años se realizará una auditoria interna o externa que verifique el cumplimiento las medidas de seguridad del Reglamento.
	Auditoria Extraordinaria	- Deberá realizarse siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.
	Informe de auditoria	- Deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. - Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas. - Los informes de auditoria serán analizados por el responsable de seguridad competente, que elevará las conclusiones al Responsable del Tratamiento para que adopte las medidas correctoras adecuadas
Gestión de soportes y documentos	Registro de entrada	Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
	Registro de Salida	Se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
Identificación y autenticación	El Responsable del Tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.	

Control de acceso físico	Exclusivamente el personal autorizado en el Registro de Actividades de Tratamiento podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.	
Registro de incidencias: recuperación de datos	- El registro deberán consignar además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. - Será necesaria la autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación de los datos.	
Gestión De soportes	Etiquetado críptico	La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
	Distribución	La distribución de los soportes se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
	Portátiles	- Se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del Responsable del Tratamiento. - Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el Registro de Actividades de Tratamiento y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.
Copias de respaldo y recuperación	Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas correspondiente, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.	
Registro de accesos	Funcionamiento	1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el Tratamiento accedido, el tipo de acceso y si ha sido autorizado o denegado. 2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. 3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. 4. El período mínimo de conservación de los datos registrados será de dos años. 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

	Excepción	No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias: a) Que el responsable del Tratamiento o del tratamiento sea una persona física. b) Que el responsable del Tratamiento o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
Tele comunicaciones	Cifrado	La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.
	Seudonimización	En cumplimiento del art. 32 del RGPD, 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.

Tratamientos No Automatizados	
Funciones y obligaciones del personal	- Definir funciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información y documentarlas en el Registro de Actividades de Tratamiento. - Definir las funciones de control o autorizaciones delegadas por el responsable del tratamiento. - Formación e información del personal para que conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento
Usuarios y control de accesos	- Acceso limitado a los recursos que el usuario precise para el desarrollo de sus funciones. - Confección de una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos. - Deben establecerse mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. - Sólo podrá conceder, alterar o anular el acceso autorizado sobre los recursos el personal autorizado para ello en el Registro de Actividades de Tratamiento, conforme a los criterios establecidos por el responsable del tratamiento. - El personal ajeno que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
Registro de incidencias	- Establecer un procedimiento de notificación y gestión de las incidencias - Establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas

Gestión de soportes y documentos	Etiquetado	- Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el Registro de Actividades de Tratamiento. - No se etiquetarán cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el Registro de Actividades de Tratamiento. - Podrán etiquetarse crípticamente (sólo comprensibles para los usuarios con acceso autorizado) cuando contengan datos de carácter personal que la organización considerase especialmente sensibles.
	Registro de salida	La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del tratamiento deberá ser autorizada por el responsable del tratamiento o encontrarse debidamente autorizada en el Registro de Actividades de Tratamiento.
	Traslado	En el traslado de la documentación se adoptarán las medidas necesarias para mantener su seguridad y asegurar la imposibilidad de acceso a personal no autorizado.
	Destrucción	Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
	Custodia de los soportes	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del tratamiento adoptará medidas que impidan el acceso de personas no autorizadas
	Dispositivos de almacenamiento	Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.
Criterios de archivo	El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En aquellos casos en los que no exista norma aplicable, el responsable del tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.	
Responsable de Seguridad	Designación	En el Registro de Actividades de Tratamiento deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.

	Tipos de designación	- Única para todos los tratamientos de datos de carácter personal. - Diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el Registro de Actividades de Tratamiento.
Auditoria	Los tratamientos no automatizados de este nivel se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad.	
Almacenamiento de la información	Armarios o archivadores	Deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el tratamiento.
	Excepción	Si, atendidas las características de los locales no fuera posible disponer de áreas cerradas el responsable adoptará medidas alternativas.
Copia o reproducción	Realización	Únicamente podrá ser realizada bajo el control del personal autorizado en el Registro de Actividades de Tratamiento.
	Destrucción	Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
Acceso a la documentación	Acceso	El acceso a la documentación se limitará exclusivamente al personal autorizado.
	Identificación	Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
Traslado de documentación	Siempre que se proceda al traslado físico de la documentación contenida en un tratamiento, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado	

8. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE LOS INTERESADOS

Para dar cumplimientoa lo establecido en la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos y Garantía de los Derechos Digitales y al Capítulo III, artículos 12 al 23 del Reglamento Europeo de Protección de Datos UE 679/2016, de 27 de Abril, del Parlamento y el Consejo (RGPD), se concretan unos modelos de formularios, que habrán de estar a disposición de los afectados para facilitarles el ejercicio de los Derechos de acceso, impugnación, rectificación, supresión, oposición, revocación del consentimiento, portabilidad, limitación del tratamiento y a presentar reclamación ante la Agencia Española de Protección de Datos.

Dichos formularios habrán de ser enviados por correo ordinario a la dirección postal ASOCIACIÓN BASIDA, CARRETERA ANTIGUA DE TOLEDO, KM. 9, 28300, ARANJUEZ, MADRID, ESPAÑA.

Igualmente podrán ejercitarse mediante el envío de correo electrónico a la dirección de email aranjuez@basida.org.

En dicho escrito habrá de justificarse la identidad del Titular que ejercita los Derechos, así como exponer brevemente las razones que lo motivan.

En todo lo no contemplado por dichos formularios, se estará a lo establecido por la legislación vigente.