REGISTRO DE ACTIVIDADES DE TRATAMIENTO

FUNDACIÓN UNIVERSIDAD DE CÁDIZ

ACTUALIZADO A MARZO DEL 2024

Fundación Universidad de Cádiz (FundUCA)
Calle Ancha 10, Edificio José Pedro Pérez-LLorca 11001, Cádiz
CIF: G-11442167 Teléfonos: 956-070370/72
www.fundacionuca.es

CONTENIDO

1. INTRODUCCIÓN

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, en adelante **RGPD**, 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) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Ambas están destinadas a proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

La Ley Orgánica 3/2018 pretende lograr la adaptación del ordenamiento jurídico español al Reglamento UE 2016/679 y, garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Ambos textos legales consideran lo siguiente:

- La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental.
- Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal, deben respetar sus libertades y derechos fundamentales.

Y garantiza:

- Un nivel uniforme y elevado de protección de las personas físicas y elimina los obstáculos a la circulación de datos personales dentro de España y de la Unión Europea.
- Un nivel coherente de protección de las personas físicas en todo el territorio UE y evitar divergencias que dificulten la libre circulación de datos personales.

2. OBJETO DEL REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El artículo 24 del RGPD establece la responsabilidad del Responsable del Tratamiento: "El Responsable del Tratamiento aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD."

Para ello, el Responsable del Tratamiento deberá tener un registro de actividades del tratamiento que contenga la información establecida en el artículo 30.1 del RGPD.

Así mismo, el artículo 28.1 de la Ley 3/2018, de 5 de diciembre, Ley Orgánica de Protección de Datos de Carácter Personal y de las garantías digitales, establece que "Los Responsables y Encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado Reglamento, con la presente Ley Orgánica, sus normas de desarrollo y la legislación sectorial aplicable."

Por tanto, es la finalidad del presente documento y sus anexos, en cumplimiento de lo dispuesto con la normativa vigente, recoger las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos de los afectados cuyos datos de carácter personal sean objeto de tratamiento.

3. ÁMBITO DE APLICACIÓN

El ámbito de aplicación del RGPD y la Ley Orgánica 3/2018, es el relativo al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero y garantizar los derechos digitales de las personas.

La protección otorgada por las citadas normativas debe aplicarse a las personas físicas, independientemente de su nacionalidad, lugar de residencia, en relación con el tratamiento de sus datos personales.

La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como su tratamiento manual, cuando los datos figuren en un fichero o estén destinados a ser incluidos en él, y garantizar los derechos digitales de las personas.

Fuera del ámbito de aplicación de estos textos legales se encuentran el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma jurídica y sus datos de contacto.

El ámbito de aplicación de éste Registro de Actividades del Tratamiento comprende a los ficheros que contienen datos de carácter personal que se hallen bajo la responsabilidad del Responsable del Tratamiento, incluyendo los sistemas de información, soportes, infraestructuras y equipos y empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los establecimientos (locales/dependencias) en los que se ubican.

4. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

Responsable	Fundación Universidad de Cádiz	Teléfono	956070370
CIF	G11442167	Correo electrónico	lopd@fundacionuca.es
Dirección	C/ Ancha 10 (Edificio José Pérez Llorca), 11001 Cádiz	Web	www.fundacionuca.es
Actividad: Entidad docente sin ánimo de lucro			

FUNCIONES y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento es el encargado jurídicamente de la seguridad de la información y por tanto de la aplicación de medidas técnicas y organizativas. Para ello, debe realizar las acciones correspondientes para que el Personal afectado por este Documento conozca las normas que aplican al desarrollo de sus funciones, para lo cual debe:

1. Implantar las medidas de seguridad establecidas en este Documento. El Responsable del Tratamiento deberá garantizar la difusión de este Documento entre todo el Personal de la Organización y todo aquel implicado.

2. Mantener el Registro de Actividad de Tratamiento actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización de este.

3. Adecuar en todo momento el contenido de este, a las disposiciones vigentes en materia de seguridad de la información.

4. Comprobar que los sistemas informáticos de acceso a los ficheros de información tengan acceso restringido, por ejemplo, mediante un código de usuario y contraseña.

5. Cuidar que todos los usuarios autorizados para acceder a los ficheros tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

6. Garantizar que el archivo de los documentos en soportes no automatizados (papel) se realice mediante criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de los interesados.

7. Autorizar expresamente la salida de soportes que contengan datos de carácter personal fuera de las dependencias del Responsable del Tratamiento.

8. Proteger el acceso a la información/documentación ubicada en soportes no automatizados (archivadores, armarios, etc..) con puertas con llave, si la sensibilidad de la información lo requiere.

9. El Responsable del Tratamiento se encargará de verificar la definición y correcta aplicación de las copias de seguridad y recuperación de los datos.

10. El Responsable del Tratamiento designará a uno o a varios Delegados de Protección de Datos, cuando así lo requiera la normativa vigente, en virtud de la dimensión, sistemática del tratamiento, sensibilidad de la información, y actividades desarrolladas por el Responsable del Tratamiento.

5. IDENTIFICACIÓN DEL TRATAMIENTO DE DATOS

TRATAMIENTO: ADMINISTRACION, FINANZAS Y CONTABILIDAD

Legitimación del tratamiento está basado en: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión económica, fiscal, contable, administrativa, facturación, cobros y pagos.

Sistema de Tratamiento: mixto.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, nº de afiliación a la Seguridad Social.
- Características personales y circunstancias sociales.
- Datos económicos: datos bancarios.
- Académicos y profesionales: Formación, titulaciones, y experiencia profesional.
- Datos empleo: Profesión, puesto de trabajo.
- Datos procedentes de sanciones administrativas.

Origen y procedencia de los datos: El propio interesado o su representante legal, estudiantes, beneficiarios, padres o tutores.

Aplicaciones: Java, Icaro y Logic. Administraciones Públicas (Agencia Tributaria).

Categorías de interesado: Estudiantes, clientes, usuarios u otros colectivos.

Las categorías de destinatarios: Universidad de Cádiz, Administración Tributaria, y otras administraciones públicas con competencia en la materia.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DEL SOPORTE TÉCNICO Y ASESORAMIENTO DE CONTENIDOS DEL CAMPUS VIRTUAL DE LA UCA

Legitimación del tratamiento: Relación contractual, el cumplimiento de obligaciones legales, y el consentimiento del interesado.

Finalidad del tratamiento: Atención de las solicitudes e incidencias del Campus Virtual de la Universidad de Cádiz.

Sistema de Tratamiento: automatizado.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, firma.
- Características personales y circunstancias sociales.
- Académicos y profesionales: Formación, titulaciones.

Origen y procedencia de los datos: datos introducidos por los usuarios del Campus Virtual de la Universidad de Cádiz.

Categorías de interesado: estudiantes y profesores.

Las categorías de destinatarios: Universidad de Cádiz.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO PARA LA GESTIÓN DE ACTIVIDADES DE PROMOCIÓN DEL EMPLEO Y PRÁCTICAS.

Legitimación del tratamiento: Relación contractual, el cumplimiento de obligaciones legales, y el consentimiento del interesado.

Finalidad del tratamiento: Atención de las solicitudes del programa de promoción del empleo de la Universidad de Cádiz.

Sistema de Tratamiento: automatizado.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, firma.
- Características personales y circunstancias sociales.
- Académicos y profesionales: Formación, titulaciones.

Origen y procedencia de los datos: datos facilitados por la Universidad de Cádiz para la ejecución del encargo.

Categorías de interesado: empresas, instituciones, estudiantes y profesores.

Las categorías de destinatarios: Universidad de Cádiz.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DE LA PROMOCIÓN DE LA INTERNACIONALIZACIÓN Y SERVICIO DE APOYO A LA GESTIÓN DE LA INTERNACIONALIZACIÓN DE TÍTULOS UCA

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión de proyectos, gestión becas y ayudas.

Sistema de Tratamiento: mixto.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, firma.
- Datos económicos.

Origen y procedencia de los datos: El propio interesado o su representante legal.

Categorías de interesado: Usuarios, alumnos.

Las categorías de destinatarios: Universidad de Cádiz y otras administraciones públicas con competencia en la materia.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DE PROYECTOS, INICIATIVAS, FORMACIÓN Y FOMENTO DEL EMPRENDIMIENTO

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Asesoramiento empresarial y colaboración entre emprendedores y agentes sociales.

Sistema de Tratamiento: La información no es almacenada.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail.

Origen y procedencia de los datos: El propio interesado o su representante legal. Entidad privada.

Categorías de interesado: Beneficiarios, solicitantes, cargos públicos, personas de contacto, estudiantes.

Las categorías de destinatarios: no se comunican datos a terceros.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LAS ACTIVIDADES DE GESTIÓN DE SUS ENSEÑANZAS PROPIAS Y SERVICIO DE APOYO A LA GESTIÓN DE PREINSCRIPCIÓN DE MÁSTERES OFICIALES

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión de las enseñanzas propias y preinscripción de Másteres Oficiales.

Sistema de Tratamiento: Automatizado.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, nº de Afiliación a la Seguridad Social, imagen.
- Datos académicos: Formación, titulaciones, historial del estudiante y experiencia profesional.
- Datos de empleo: profesión, puesto de trabajo, datos no económicos de la nómina, historial del trabajador, vida laboral, nóminas, situación de empleo o desempleo.
- Datos económicos: datos bancarios.

Origen y procedencia de los datos: El propio interesado o su representante legal. Aplicaciones JAVA, DUA, CERVANTES y otras aplicaciones.

Categorías de interesado: Alumnos, estudiantes, usuarios u otros colectivos.

Las categorías de destinatarios: Universidad de Cádiz, organizaciones o personas directamente relacionadas con el responsable.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DEL CENTRO SUPERIOR DE LENGUAS MODERNAS (CSLM)

Legitimación del tratamiento: Relación contractual, el cumplimiento de obligaciones legales, y el consentimiento del interesado.

Finalidad del tratamiento: Atención de solicitudes del programa de inmersión lingüístico cultural en familias dentro del programa de acogida en hogares de estudiantes extranjeros en programas convenidos con universidades extranjeras en el CSLM. Atender y gestionar las solicitudes de admisión para el alojamiento en las residencias de estudiantes. Gestión de la formación del Centro Superior de Lenguas Extranjeras.

Sistema de Tratamiento: automatizado.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail, firma.
- Características personales y circunstancias sociales.
- Académicos y profesionales: Formación, titulaciones.
- Datos de salud: Diabético, asma, intolerancia, alergias, tratamientos médicos, otro tipo de información médica.

Origen y procedencia de los datos: El propio interesado o su representante legal y de la propia familia. Aplicaciones Java. Universidad. Propio docente.

Categorías de interesado: estudiantes.

Las categorías de destinatarios: Universidad de Cádiz.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DE LA RESIDENCIA UNIVERSITARIA "LA CALETA"

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión y atención de solicitudes de alojamiento en la Residencia Universitaria.

Sistema de Tratamiento: mixto.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, teléfonos, e-mail.
- Características personales y circunstancias sociales.
- Académicos y profesionales: formación, titulaciones, historial del estudiante.
- Datos de económicos: renta e ingreso de los padres.

Origen y procedencia de los datos: El propio interesado o su representante legal.

Categorías de interesado: estudiantes.

Las categorías de destinatarios: Universidad de Cádiz.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: RECURSOS HUMANOS

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión de la relación laboral con los empleados. Gestión de nóminas, selección de personal, facturación. Gestión de las profesiones, gestión de prácticas y facturación.

Sistema de Tratamiento: mixto.

Descripción de las categorías de empleados y de las categorías de datos personales: Empleados. Personas que trabajan para el responsable del tratamiento.

Categorías de datos personales: Gestión de nóminas, elaboración de los seguros sociales, recursos humanos.

- De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail.
- Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía.
- Datos académicos. Datos profesionales.
- Datos bancarios, para la domiciliación del pago de las nóminas.

- Datos procedentes de sanciones administrativas.

Origen y procedencia de los datos: El propio interesado o su representante legal.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales: Bancos y entidades financieras. Administración de la Seguridad Social. Gestoría Laboral.

Los plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LAS ACTIVIDADES DE GESTIÓN DE LA ESCUELA INFANTIL LA ALGAIDA

Legitimación del tratamiento: Relación contractual y el cumplimiento de obligaciones legales.

Finalidad del tratamiento: Gestión Escuela Infantil. Gestión de los alumnos matriculados en la escuela infantil.

Sistema de Tratamiento: mixto.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail.
- Características personales y circunstancias sociales.
- Académicos.
- Datos de salud.

Origen y procedencia de los datos: El propio interesado o su representante legal. Padres o tutores.

Categorías de interesado: Estudiantes, padres o tutores

Las categorías de destinatarios: organizaciones o personas relacionadas directamente con el responsable. Administración pública.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: RECLAMACIONES (EXPONE/SOLICITA)

Legitimación del tratamiento: cumplimiento de obligaciones legales.

Finalidad del tratamiento: En la recogida de las observaciones que pueda realizar los usuarios de la Fundación.

Sistema de Tratamiento: manual.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, teléfonos, e-mail.

Origen y procedencia de los datos: El propio interesado o su representante legal.

Categorías de interesado: Usuarios.

Las categorías de destinatarios: Universidad de Cádiz, docentes y el interesado.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: REGISTRO DE ENTRADA Y SALIDA DEL CORREO POSTAL

Legitimación del tratamiento: cumplimiento de obligaciones legales.

Finalidad del tratamiento: Registro de entrada y salida de documentación presentada en la Fundación.

Sistema de Tratamiento: Manual.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail.

Origen y procedencia de los datos: El propio interesado o su representante legal. Datos procedentes de sanciones administrativas.

Categorías de interesado: Solicitantes, usuarios, beneficiarios, estudiantes.

Las categorías de destinatarios: no se comunican datos a terceros.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

TRATAMIENTO: SERVICIO DE APOYO A LA GESTIÓN DE ENCUESTAS DE SATISFACCIÓN DE GRUPOS DE INTERÉS

Legitimación del tratamiento: cumplimiento de obligaciones legales.

Finalidad del tratamiento: Recogida de información de la satisfacción de los estudiantes, tutores externos, PDI, PAS, egresados, empleadores. Contratación de los servicios y suministros necesarios para el desarrollo de la actividad. Evaluación de la satisfacción de grupos de interés.

Sistema de Tratamiento: Mixto.

Descripción de las categorías de datos personales:

- De identificación: nombre y apellidos, NIF, teléfonos, e-mail.
- Datos de empleo: Profesión, puesto de trabajo.

Origen y procedencia de los datos: El propio interesado o su representante legal. Aplicaciones de la UCA.

Categorías de interesado: usuarios y docentes.

Las categorías de destinatarios: Universidad de Cádiz.

Plazos previstos para la supresión de las diferentes categorías de datos: Los previstos por la legislación respecto a la prescripción de responsabilidades.

6. MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LOS NIVELES DE SEGURIDAD ADECUADOS AL RIESGO

Conforme al art. 32 del RGPD y art.28 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantías de los derechos digitales, para la seguridad del tratamiento, establece lo siguiente:

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 riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado de seguridad al riesgo, que, en su caso, incluya, entre otros:

- La seudonimización y el cifrado de los datos.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes 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.

6.1. Medidas y normas relativas a la identificación del personal autorizado a acceder a los datos personales

CONTROL DE ACCESO A FICHEROS AUTOMATIZADOS

- Los sistemas informáticos que contienen los ficheros deberán tener su acceso restringido mediante un código de usuario y una contraseña.

- Debe existir una relación actualizada de usuarios que sólo será conocida por el propio usuario.
- 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.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Exclusivamente el administrador está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del tratamiento.
- Los equipos informáticos deberán contar con antivirus y firewalls.
- Los sistemas operativos de los equipos informáticos deberán estar actualizados.
- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información limitando el número máximo de intentos fallidos. Cuando sea técnicamente posible, se guardará en un fichero auxiliar la fecha, hora, código y claves erróneas que se han introducido, así como otros datos que ayuden a descubrir la autoría de esos intentos de acceso no autorizados en los ficheros. (Medida de seguridad para datos sensibles).

Adjuntar los Procedimientos de Identificación y autentificación de Usuarios (PR005)

REGISTRO DE ACCESOS A FICHEROS AUTOMATIZADOS

- De cada acceso al fichero se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si se trata de un acceso autorizado, será preciso guardar la información que permita identificar el registro accedido. (Medida de seguridad para datos sensibles).
- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable del tratamiento sin que se deba permitir, en ningún caso, la desactivación de los mismos. (Medida de seguridad para datos sensibles).
- El periodo de conservación de los datos registrados será mínimo de dos años.
- El registro de accesos deberá ser revisado por el responsable del tratamiento o si procede por el DPO.

PROCEDIMIENTO DE ASIGNACIÓN DE CONTRASEÑA

- Las contraseñas se asignarán y cambiarán mediante un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.
- La periodicidad del cambio de contraseñas serán inferior a un año.
- Las contraseñas deberán ser suficientemente complejas y seguras, evitando el uso propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc. Para ello se seguirán las siguientes pautas en la elección de las contraseñas:
    1. Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
    2. No deberán coincidir con el código de usuario.
    3. No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario (nombre, apellidos, ciudad y fecha de nacimiento, DNI, nombre de familiares, matrícula del coche, etc.).
- Las contraseñas deberán ser estrictamente confidenciales y personales. Cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible. Deberá registrarse como incidencia y proceder inmediatamente a su cambio.
- El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Adjuntar el Procedimiento de Asignación y gestión de contraseñas (PR010)

CONTROL DE ACCESO FÍSICO A LOCALES

- Los locales donde se ubiquen los ordenadores o archivos que contienen los ficheros deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos.
- Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad de los ficheros que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

- Exclusivamente el personal autorizado podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Adjuntar el Procedimiento de Control de acceso físico (PR012)

CONTROL DE ACCESO A FICHEROS NO AUTOMATIZADOS (EN PAPEL)

- El responsable del tratamiento se encargará de que exista una relación actualizada de usuarios con acceso a ficheros no automatizados.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- La empresa de limpieza, así como cualquier otra empresa prestataria de servicios garantizarán la observancia de las medidas de seguridad necesarias para que no se produzca, voluntaria o involuntariamente, incidencia alguna en las dependencias del responsable del tratamiento, siendo aquella responsable de las que se produzcan.
- Iguales garantías se deberán adoptar en el desarrollo de las obras y tareas de mantenimiento y reparación de los elementos ubicados dentro de las dependencias del responsable del tratamiento.
- Se establecerá un control de los accesos autorizados, pudiendo exclusivamente los usuarios autorizados acceder a los ficheros no automatizados.
- El acceso de personas no incluidas en el Anexo de Personal Autorizado deberá adecuadamente registrado.

6.2. Gestión y almacenamiento de soportes y documentos

FICHEROS AUTOMATIZADOS

Un soporte es un objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado.
- La información contenida en los soportes informáticos deberá estar cifrada.
- Los soportes se almacenarán en un lugar con acceso restringido, para que su utilización quede restringida a las personas con acceso autorizado a los ficheros.
- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.
- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del tratamiento.
- Se confeccionará un inventario de soportes que contendrá la siguiente información respecto de cada soporte inventariado: tipo de soporte, fecha de su creación, información que contiene y lugar donde se encuentra almacenado. El inventario se mantendrá constantemente actualizado.
- Cuando los soportes informáticos vayan a salir de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.
- Deberá establecerse un sistema de registro de entrada de soportes que permita conocer el tipo de documentos, la fecha, hora, el emisor, el número de soportes y la personal responsable de la recepción que deberá estar debidamente autorizada.
- La distribución de los soportes se realizará del siguiente modo:
    - Los soportes serán almacenados con un sistema de etiquetado confidencial.
    - La distribución de los soportes se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte, evitándose el uso de los dispositivos que no permitan cifrado o la adopción de medidas alternativas.
    -

FICHEROS NO AUTOMATIZADOS

- El responsable del tratamiento contará con dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.
- El archivo de los documentos se realizará garantizando que los documentos van a estar perfectamente conservados, y sea fácil localizar y consultar su información. Todo ello para posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y supresión.
- Cuando los documentos con datos personales no se encuentren archivados en las carpetas u otros dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren al cargo de estos deberán custodiarlos e impedir en todo momento que pueden ser una documentación a la que tenga acceso personal no autorizado.
- Se utilizarán armarios cerrados con llave en los que los datos estarán dispuestos con un criterio lógico en los archivadores. Siendo responsabilidad del responsable del tratamiento el impedir el acceso a la información por personas no autorizadas.
- Deberá establecerse un sistema de registro de entrada y salida de documentos que permita conocer el tipo de información contenidas, la fecha, hora, el emisor, el número de documentos y la personal responsable de la entrada y salida.
- La entrada o salida de documentos debe estar autorizada por el responsable del tratamiento.

6.3. Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Los datos personales que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizarán previamente cifrando los datos por los distintos mecanismos de cifrado que se utilicen y garanticen que la información no va a ser inteligible ni manipulada por terceros.

6.4. Régimen de trabajo fuera de los locales

FICHEROS AUTOMATIZADOS

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del tratamiento y, en todo caso, deberá garantizarse las medidas de seguridad.

En la autorización para el tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá aparecer lo siguiente:

- Finalidad para la cual se solicita la autorización.
- Tipo de tratamiento (automatizado, no automatizado, mixto)
- Tipo de dispositivo portátil (en su caso)
- Tipo de documentación objeto de tratamiento
- Ficheros de dónde proceden los datos
- Periodo de validez de la autorización
- Medidas de seguridad implementadas para proteger la información
- Persona autorizada para trabajar fuera de los locales
- Cargo/departamento
- Observaciones
- Firma de la persona que autoriza

El tratamiento fuera de los locales de trabajo deberá cifrarse los datos que contengan los dispositivos portátiles cuando éstos se encuentran fuera de las instalaciones que están bajo control del responsable del tratamiento.

Se deberá evitar el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado.

FICHEROS NO AUTOMATIZADOS

- Siempre que se proceda al traslado físico de la documentación contenida en un fichero se trasladará con la debida diligencia y cuidado, para impedir su pérdida en el desplazamiento.

- En los ficheros no automatizados se adoptarán medidas que impidan el acceso o manipulación, tales como la utilización de un maletín con cierre de seguridad para trasladar los documentos.

6.5. Procedimiento para la realización de copias de reproducción

- Deberán realizarse copias de seguridad periódicamente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
- Los procedimientos establecidos para la realización de copias de seguridad y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
- El responsable del tratamiento se encargará de verificar cada seis meses, la definición y correcta aplicación de los procedimientos de realización de copias de seguridad y de recuperación de los datos.
- Será necesaria la autorización por escrito del responsable del tratamiento para la ejecución de los procedimientos de recuperación de los datos.
- Deberá conservarse una copia de seguridad y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos.
- Las copias desechadas deberán ser destruidas, imposibilitando el posterior acceso a la información contenida en los documentos.

Adjuntar el Procedimiento de Copias de Seguridad (PR009)

6.6. Telecomunicaciones de categorías de datos sensibles

Todas las entradas y salidas de datos del fichero que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el Responsable del tratamiento. Igualmente, si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos de los ficheros, en directorios protegidos y bajo el control del responsable citado. Se mantendrán copias de esos correos durante al menos dos años. También se guardará durante un mínimo de dos años, en directorios protegidos, una copia de los ficheros recibidos o transmitidos por sistemas de transferencia de ficheros por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino del fichero enviado.

Cuando los datos de los Ficheros vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean encriptados de forma que solo puedan ser leídos e interpretados por el destinatario.
La transmisión de datos a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

7. PROCEDIMIENTO DE REVISIÓN DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS RECOGIDAS EN ESTE DOCUMENTO

Según establece el artículo 30 del RGPD *"El responsable o encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite"*

Por tanto, es fundamental que este documento esté permanentemente actualizado, y en un formato claro y legible que facilite su compresión por parte de terceros. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de estos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la documentación total o parcial.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.

8. IDENTIFICACIÓN DEL ENCARGADO DEL TRATAMIENTO

En el Considerando 81 del RGPD establece que *"respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular, en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.*

El tratamiento por un encargado debe regirse por un contrato, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los interesados."

El artículo 28.1 del RGPD establece que *"cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente a un encargado de tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con el Reglamento."*

En cumplimiento del artículo 28.3 del RGPD se deberá formalizarse un contrato de acceso a datos, de manera que acredite fehacientemente su celebración y contenido.

LISTADO DE CONTRATOS DE TRATAMIENTO DE DATOS

Contratos de Tratamiento de Datos		
Entidad	Servicio prestado	Fecha del contrato
Ozonia Consultores, S.L.	Asesoramiento en protección de datos	

8. DELEGADO DE PROTECCIÓN DE DATOS

El responsable del tratamiento designará un delegado de protección de datos encargado de coordinar y controlar las medidas definidas en este documento.

El delegado de protección de datos desempeñará las funciones:

- Informar y asesorar al responsable del fichero y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento Europeo de Protección de Datos y la normativa española.
- Supervisar el cumplimiento de lo dispuesto en el Reglamento Europeo y la normativa española, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorias correspondientes.
- Ofrecer asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas sobre cualquier otro asunto.

El Registro de nombramiento/s de Delegado/s de Protección de Datos es el siguiente:

Razón Social o Nombre y Apellidos	**CIF/DNI**	**Correo Electrónico**	**Teléfono**	**Fecha de Alta**	**Fecha de Baja**	**Fecha de comunicación en la AEPD**
OZONIA CONSULTORES, S.L.	B11490083	VSV@OZONIA.ES	910053122	17/11/20		17/11/20

9. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Todos los usuarios deben conocer sus funciones y obligaciones en cuanto al RGPD y Ley Orgánica 3/2018 de Protección de Datos y garantías de los derechos digitales.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de estas, serán informadas de acuerdo con siguiente procedimiento:

1. Se facilitará una copia del ANEXO de FUNCIONES Y OBLIGACIONES DEL PERSONAL a cada usuario con acceso a los ficheros, o, en su defecto, se tendrá siempre a su disposición para cualquier consulta.
2. Se firmará por cada usuario el DOCUMENTO DE CONFIDENCIALIDAD, incorporando estos documentos al mismo.
3. Se facilitará la Política de los Recursos Informáticos a cada usuario con acceso a los ficheros que contienen información personal.
4. Se facilitará la Política de Desconexión Digital.

10. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

Se considera como violación de la seguridad de los datos personales aquella violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

NOTIFICACIONES

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos del interesado. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

La notificación contemplada deberá contener como mínimo:

- Describir 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 aproximados de registros de datos personales afectados.
- Comunicar el nombre y los datos de contacto del delegado de protección de datos u otro contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.
- El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento.

11. PROCEDIMIENTO DE EJERCICIOS DE DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, OPOSICIÓN, LIMITACIÓN AL TRATAMIENTO Y PORTABILIDAD DE LOS DATOS.

El RGPD otorga a los interesados cuyos datos sean tratados y obren en ficheros los siguientes derechos:

1. Derecho de acceso
2. Derecho de rectificación
3. Derecho de supresión
4. Derecho de oposición.
5. Derecho a la limitación del tratamiento.
6. Derecho a la portabilidad de los datos.

El Responsable del Tratamiento debe arbitrar fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del RGPD, incluidos mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales, y su rectificación o supresión, así como el ejercicio del derecho de oposición.

A continuación, se exponen los protocolos de actuación a seguir para la correcta cumplimentación de tales solicitudes.

1. Derecho de acceso

El interesado tiene derecho a solicitar y obtener gratuitamente información de los datos de carácter personal sometidos a tratamiento:

- Los fines del tratamiento,
- Las categorías de datos personales que se trate,
- Los destinatarios o las categorías de destinatarios,
- De ser posible el plazo previsto de conservación,

- La existencia del derecho a solicitar del responsable la rectificación o supresión de los datos personales o la limitación del tratamiento de datos personales,
- Derecho a presentar una reclamación ante la autoridad de control.

Este derecho sólo puede ser ejercitado a intervalos no inferiores a doce meses (salvo que se acredite por el interesado un interés legítimo para ejercitarlo antes de que transcurra un año desde la última vez que hizo uso del derecho).

En el momento en que se reciba un escrito solicitando ejercer el derecho de acceso, los pasos a seguir serán los siguientes:

- Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
- Contestación al interesado en plazo facilitando una copia de los datos personales objeto de tratamiento.

2. y 3. Derechos de rectificación y supresión

En el caso de que se reciba una solicitud de rectificación es importante que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento, la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos.

En el caso de que se reciba una solicitud de supresión, el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales

En el momento en que se reciba un escrito solicitando ejercer el derecho de rectificación o supresión, los pasos a seguir serán los siguientes:

Solicitud de rectificación

- Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.

- Contestación al interesado en plazo.

Solicitud de supresión

- Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
- El Responsable del Tratamiento deberá suprimir sin dilación los datos personales del interesado.

4. Derecho de oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el art. 6. 1, letras e) o f), incluida la elaboración de perfiles.

El Responsable del Tratamiento dejará de tratar los datos personales, salvo que acredita motivos legítimos imperiosos para el tratamiento prevalezcan sobre los interesados.

Solicitud de oposición

- Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
- El Responsable del Tratamiento dejará de tratar sin dilación los datos personales del interesado.

5. Derecho a la limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos.
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.

- El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- El interesado se haya opuesto al tratamiento en virtud del art. 21. 1 del RGPD.

6. Derecho a la portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.

12. PROCEDIMIENTO DE CONSERVACIÓN Y SUPRESIÓN DE LOS DATOS

El Procedimiento de conservación y supresión de datos personales, pretende establecer unas directrices de actuación relativas a determinar cuándo debe procederse a la conservación o a la destrucción de los datos, a los efectos de dar cumplimiento a las exigencias derivadas del deber de calidad.

La presente Política deberá ser observada por el RESPONSABLE DEL TRATAMIENTO y por todo el personal que maneje datos de carácter personal en el desarrollo de su actividad.

OBLIGACIONES DE SUPRESIÓN DE DATOS PERSONALES

1. Consideraciones previas

Según los principios recogidos en el art. 5 del Reglamento (EU) de 2016/679 de Protección de Datos Personales, los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el Responsable del Tratamiento ha de establecer plazos para su supresión o revisión periódica.

A tal efecto, la presente Política debe guiarse por Principio de limitación del plazo de conservación del apartado e) del artículo 5.1 del RGPD, en virtud del cual los datos personales deben ser "*mantenidos de*

forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales."

2. **Causas habilitantes de la supresión de los datos personales**

2.1 Terminación de la condición legitimadora del tratamiento.

Cuando los mismos ya no sean útiles ni necesarios para la finalidad que justificó su recogida y tratamiento, o una vez cumplida y agotada dicha finalidad deberá procederse a la supresión de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los mismos para responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las mismas previstas en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

2.2 Ejercicio del derecho de supresión

Cuando el interesado ejerza el derecho de supresión de los datos personales, siempre que concurran alguna de las circunstancias siguientes:

1. los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
2. el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico;
3. el interesado se oponga al tratamiento con arreglo al artículo 21.1 del RGPD (derecho de oposición), y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento cuando éste tenga por objeto la mercadotécnica directa (artículo 21.2 del RGPD);
4. los datos personales hayan sido tratados ilícitamente;
5. los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

6. los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños, mencionados en el artículo 8.1 del RGPD.

En estos casos, deberá procederse a la eliminación de los datos personales, siempre y cuando no sea necesario proceder al bloqueo de los ismos para responder ante posibles responsabilidades derivadas del tratamiento de datos personales y por el plazo de prescripción de las ismas previstas en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

No obstante lo anterior, no se aplicará el derecho de supresión, y por tanto los datos podrán continuar siendo tratados por el responsable del tratamiento cuando el tratamiento sea necesario:

7. para ejercer el derecho a la libertad de expresión e información;

8. para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

9. por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

10. con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

11. para la formulación, el ejercicio o la defensa de reclamaciones.

MECANISMOS DE SUPRESIÓN DE LOS DATOS PERSONALES

- Si los datos están contenidos en soporte no automatizado, se deberá proceder a la destrucción física de los documentos. A tal efecto se recomienda:

    - La utilización de proveedores de servicio de destrucción documental

- La utilización de herramientas de destrucción física de papel, tal y como, destructoras de papel.

- Opcionalmente, y en el caso en que la supresión tenga como origen el ejercicio de derecho de supresión, la supresión podrá tener lugar mediante la entrega de dicha información a la persona o personas que sean titulares de esta.

- Si los datos están contenidos en soporte informático, se procederá de igual forma a su eliminación física de la aplicación, sin que sea suficiente el empleo de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren los derechos de supresión.

PLAZOS LEGALES DE CONSERVACIÓN DE DATOS

En los casos en los que exista obligación legal de conservar los datos durante un periodo de tiempo determinado y/o durante los plazos de prescripción de las acciones que pudieran derivarse de la actividad o servicio prestado, el RESPONSABLE DEL TRATAMIENTO DE DATOS procederá al bloqueo de los datos durante los referidos plazos.

Los datos bloqueados quedarán, únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas y/o durante los plazos legales establecidos al efecto. Cumplidos los indicados plazos, deberá procederse a la supresión de los datos bloqueados.

El bloqueo de los datos consiste en la identificación y reserva de estos, adoptando medidas técnicas, organizativas, para impedir su tratamiento, incluyendo si visualización.

Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada anteriormente.

En caso de que, para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo de los datos o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, fecha del bloqueo y la no manipulación de los datos durante el mismo.

Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica, en cada caso, para cada actividad de tratamiento.