SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E.

# MANUAL DE TRATAMIENTO DE DATOS PERSONALES CONFORME AL REGLAMENTO(UE) 2016/679 Y LEY ORGÁNICA 3/2018

Sistema de Protección de Datos

**Código:** RGPD.MAN.001
**Versión:** 4.0
**Fecha:** 11/04/2023
**Nivel**: USO INTERNO

## Revisión y aprobación

| Elaboración | Revisión | Aprobación |
|---|---|---|
| Delegada de Protección de Datos.<br>MEDINA FERNANDEZ MARIA BEGOÑA - 11799130S<br>Firmado digitalmente por MEDINA FERNANDEZ MARIA BEGOÑA - 11799130S<br>Fecha: 2023.04.19 10:15:06 +02'00'<br>11/04/2023 | Directora de la asesoría jurídica y secretaria general<br>COTO DEL VALLE CRISTINA - 10878071Z<br>Firmado digitalmente por COTO DEL VALLE CRISTINA - 10878071Z<br>Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-10878071Z, givenName=CRISTINA, sn=COTO DEL VALLE, cn=COTO DEL VALLE CRISTINA - 10878071Z<br>Fecha: 2023.04.19 11:50:26 +02'00' | Secretaria del Consejo de Administración<br>COTO DEL VALLE CRISTINA - 10878071Z<br>Firmado digitalmente por COTO DEL VALLE CRISTINA - 10878071Z<br>Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-10878071Z, givenName=CRISTINA, sn=COTO DEL VALLE, cn=COTO DEL VALLE CRISTINA - 10878071Z<br>Fecha: 2023.04.27 11:27:10 +02'00' |

## Control de versiones

| Versión | Fecha | Páginas | Descripción |
|---|---|---|---|
| 1.0 | 01/10/2018 | todas | Versión Inicial |
| 2.0 | 01/02/2019 | todas | Adaptación Ley 0rgánica 3/2018 |
| 3.0 | 04/02/2021 | todas | Integración con SG-ENS |
| 4.0 | 11/04/2023 | todas | Actualización |

## Propiedad del documento

## Índice de contenido

## 1. OBJETO

El objeto de este documento es recoger todos los elementos iniciales requeridos para dar cumplimiento a la normativa de protección de datos, definiendo y estableciendo aspectos esenciales, para mantener la diligencia debida del responsable.

A todos los efectos este documento da cumplimiento al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento o Reglamento General de Protección de Datos o RGPD) y a la Ley Orgánica 3/ 2018, de 5 diciembre , de Protección de Datos Personales y Garantía de los Derechos Digitales ( en adelante LOPD o LOPDPGDD).

## 2. ALCANCE

El presente documento es de aplicación a toda la organización (personas, procesos y sistemas de información) que se encuentre dentro del ámbito de aplicación del Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales. Se ha de considerar que un Sistema de Información es el conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, poner a disposición, presentar o transmitir.

Quedan afectadas SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E, y las sociedades incluidas en el grupo, AGRUMINSA, S.A., S.M.E, A.I. ABRA INDUSTRIAL, S.A., S.M.E, PARQUE EMPRESARIAL PRINCIPADO DE ASTURIAS, S.L., S.M.E, VIPAR PARQUE EMPRESARIAL, S.L., S.M.E, PARQUE EMPRESARIAL DE CANTABRIA, S.L., SOCIEDAD PARA EL DESARROLLO INDUSTRIAL DE EXTREMADURA, S.A. S.M.E (SODIEX), SEPIDES GESTIÓN, S.G.E.I.C., S.A. S.M.E., ESPACIOS ECONÓMICOS EMPRESARIALES, S.L. Y LA SOCIEDAD ESTATAL DE MICROELECTRÓNICA Y SEMICONDUCTORES, S.A., S.M.E.

Con independencia de que el presente manual aplique a todas las empresas del Grupo SEPIDES, cada una de ellas es responsable del tratamiento de sus propios datos.

## 3. REFERENCIAS DOCUMENTALES

| Documentación Interna | Documentación Externa |
|---|---|
| | |
| | |
| | |
| | |

## 4. GLOSARIO DE TÉRMINOS

En el presente documento se han utilizado las siguientes abreviaturas y definiciones:

**AEPD**: Autoridad de Control – Agencia Española de Protección de Datos.

**ANÁLISIS DE RIESGOS**. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

**ANONIMIZACIÓN:** Proceso por el que se elimina o reduce al mínimo el riesgo de reidentificación de las personas y estos datos podrían almacenarse o tratarse, por ejemplo, para fines estadísticos.

**BARRIDO DE PUERTOS:** O escaneo de puertos, es una técnica usada por administradores para auditar máquinas y redes con el fin de saber que puertos están abiertos o cerrados, los servicios que son ofrecidos, chequear la existencia de un firewall, así como verificaciones sobre el funcionamiento. Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos.

**CEPD**: Comité Europeo de Protección de Datos

**CERTIFICADO DIGITAL:** También llamado certificado electrónico, es un fichero informático realizado por una entidad de servicios de certificación que relaciona datos de identidad a una empresa o persona física confirmando su identidad digital en Internet.

**CLOUD O "COMPUTING CLOUD"**: (Computación en la nube), es el nombre que se le dio al procesamiento y almacenamiento masivo de datos en internet, facilitando el acceso desde cualquier dispositivo electrónico con acceso a internet.

**COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:** Órgano colegiado que coordina las actividades de la organización en materia de seguridad de la información

**CORREO ELECTRÓNICO**: Todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo.

**DATOS PERSONALES:** Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

**DPD/DPO**: Delegado de Protección de Datos.

**EIPD:** Evaluación de Impacto en Protección de Datos. Antes de llevar a cabo cualquier tratamiento que presente un riesgo específico a la privacidad de acuerdo con su naturaleza, alcance o propósitos.

**ELABORACIÓN DE PERFILES:** Cualquier forma de tratamiento automatizado de datos personales con la intención de evaluar ciertos aspectos personales correspondientes a persona física, o analizar o predecir en particular el rendimiento de la persona en su trabajo, su situación económica, ubicación, salud, preferencias personales, confiabilidad, o su comportamiento.

**ENS**: Esquema Nacional de Seguridad.

**FIREWALL:** O cortafuegos (firewall) es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Forma parte de un

sistema o una red, diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

**HOSTING**: Es un servicio para almacenamiento de información y datos en un espacio en sus servidores. Este servicio puede ser de pago o gratuito.

**IP(s):** Internet Protocolo, Protocolo de Internet. Número de identificación de una Interfaz en red para un dispositivo. Sirven para identificar a un dispositivo conectado a Internet u otra red. La IP será fija o dinámica en función de si siempre es la misma o si puede ir cambiando. Normalmente son asignadas por el proveedor de acceso a Internet, un Router o el administrador de la red. Ambas IP son afectadas por la normativa de protección de datos.

**MEMORIA USB "UNIVERSAL SERIAL BUS":** También denominada lápiz de memoria, lápiz USB, memoria externa o pendrive, es un dispositivo de almacenamiento de datos que utiliza memoria flash para guardar toda la información.

**OFUSCACIÓN:** Proceso de ocultar o dificultar el acceso a la información mediante técnicas de camuflaje, encriptación, compresión, etc.

**PROTOCOLOS DE SEGURIDAD (SSL):** Secure Socket Layer. Protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación, lo que garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por elementos no autorizados, garantizando de esta forma que sólo los emisores y los receptores legítimos sean los que tengan acceso a la comunicación de manera íntegra.

**RESPONSABLE DE SEGURIDAD:** El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Persona encargada de velar por la seguridad de la información de la organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la información, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología.

**RESPONSABLE DE SISTEMAS:** Persona responsable de los servicios e infraestructura tecnológica de la entidad, con capacidad para operar sobre los sistemas, mantener comunicaciones con proveedores tecnológicos y gestionar las instalaciones, software y hardware.

**RGPD**: Reglamento General de Protección de Datos.

**SEGREGACIÓN DE FUNCIONES:** La separación o segregación de funciones es una regla básica en los controles: evitar que una persona pueda dominar todo un proceso, o tenga acceso a funciones o tareas que no requiere. Se requiere la separación de tal forma que errores u omisiones, o incumplimientos de controles de seguridad, puedan ser identificados.

**SEGURIDAD POR DEFECTO:** El uso ordinario del sistema es sencillo y seguro, de forma que una utilización insegura requiere de un acto consciente por parte del usuario.

**SEPD:** Supervisor Europeo de Protección de Datos

**SERVIDOR:** Es una computadora central que forma un sistema de red, éste provee servicios y programas a otras computadoras conectadas.

**SEUDONIMIZACIÓN:** Los datos son anonimizados si no incluyen identificadores; en cambio, son pseudonimizados si los identificadores están cifrados. A diferencia de los datos anonimizados, los datos pseudonimizados son datos personales.

**SOLUCIONES TI:** Son un conjunto de software o aplicaciones informáticas que facilitan la gestión y administración.

**SOPORTE INFORMÁTICO O AREA TI O DEPARTAMENTO DE TI:** Es un servicio que ofrecen especialistas en apoyo técnico y de este modo proporcionan asistencia técnica y asesoramiento a clientes que dependen de puntos tecnológicos.

**TERCERO:** Cualquier persona física o legal, autoridad pública, agencia, o cualquier otra entidad diferente al interesado, responsable, encargado y de las personas que, bajo la autoridad directa del responsable o encargado, están autorizadas a tratar los datos.

**USUARIO**: Persona física que utiliza con fines privados o empresariales o para el sector público un servicio de comunicaciones electrónicas o un servicio informático o de tecnología, incluyendo el acceso a la red interna o a aplicaciones destinadas a la gestión de funciones laborales o de función pública.

**VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES**: Toda 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

**VMWARE (APPLIANCE VIRTUAL VCENTER): C**omponente que permite gestionar centralizadamente múltiples servidores bajo VMware vSphere ESXi y máquinas virtuales.

**VMWARE:** Es un sistema de virtualización por software. Programa que consigue simular un sistema físico con características de hardware determinadas.

**VPN ACCESO REMOTO:** Es la empleada para proteger las comunicaciones entre un equipo individual de usuario y la red interna de la organización. Normalmente se emplean para los usuarios que trabajan desde casa o que están de viaje, y que requieren de un acceso a los recursos internos de la organización, a través de la infraestructura proporcionada por una red pública, como por ejemplo Internet.

**VPN:** Red privada virtual, es un tipo de tecnología conectada a la red que permite seguridad en la red local cuando el aparato está conectado a internet**.** Proporciona conexiones virtuales seguras, construidas sobre una red física no segura (normalmente una red pública, como por ejemplo Internet). La VPN proporciona múltiples mecanismos de seguridad que aportan la protección y el control necesario a la información transmitida. Los mecanismos de seguridad de las VPN, están destinados a preservar la confidencialidad, integridad, autenticación, ofrecer protección frente a reenvíos, y proporcionar control de acceso de las comunicaciones.

**WIFI**: Es un mecanismo de conexión inalámbrica a dispositivos electrónicos. Los dispositivos habilitados con WIFI pueden conectarse a Internet a través de un punto de acceso de red inalámbrica.

## 5. POLÍTICA DE SEGURIDAD Y PROTECCIÓN DE DATOS

SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E, en el marco de su programa estratégico de cumplimiento legal y seguridad de la información, ha considerado necesario gestionar la seguridad de su sistema de información, incluyéndose los datos personales, de manera integral y transversal, considerando en todo caso, el conjunto de las sociedades que integran el grupo, AGRUMINSA, S.A., S.M.E, A.I. ABRA INDUSTRIAL, S.A., S.M.E, PARQUE EMPRESARIAL PRINCIPADO DE ASTURIAS, S.L., S.M.E, VIPAR PARQUE EMPRESARIAL, S.L., S.M.E , PARQUE EMPRESARIAL DE CANTABRIA, S.L., SOCIEDAD PARA EL DESARROLLO INDUSTRIAL DE EXTREMADURA, S.A. S.M.E (SODIEX), SEPIDES GESTIÓN, S.G.E.I.C., S.A. S.M.E , ESPACIOS ECONÓMICOS EMPRESARIALES, S.L. Y LA SOCIEDAD ESTATAL DE MICROELECTRÓNICA Y SEMICONDUCTORES, S.A., S.M.E. Cuando a lo largo de la presente política, se haga referencia a la palabra organización, se hará en relación con el conjunto de entidades integradas en el grupo SEPIDES.

Todos los procesos internos y externos quedan adscritos y afectos, a la presente política de seguridad, y a cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

La Dirección ha considerado la seguridad en cada etapa del ciclo de vida del sistema y de la información, desde el diseño de un servicio hasta su retirada, incluyendo las diferentes fases de desarrollo o adquisición y la propia producción o explotación. Se consideran incluidos en el ciclo de vida, los proveedores y servicios externalizados, que estarán sometidos a este ciclo de vida.

Esta política ha considerado las necesidades de la parte de la información sometida a una normativa estricta, el RGPD y la LOPD. Esta política ha de ser considerada como Política de Protección de Datos, y está alineada con la Política de Seguridad. La organización ha considerado la necesidad de conciliar las distintas normas que impactan en el sistema de información, por lo que se considerara la seguridad declarada por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante RD 311/2022).

El sistema está diseñado para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad. El sistema ha considerado, los objetivos de la organización, el marco regulatorio y legal implicado y en vigor, los roles y funciones de seguridad asociadas, la coordinación de seguridad y la mejora continua.

Por defecto, la Dirección ha considerado que la entidad es el responsable de los activos de información y de los recursos de su propiedad, y asume que las tareas relacionadas con la seguridad de la información son una parte fundamental para el desarrollo de negocio. Como activo de información se ha considerado el dato personal en toda su extensión.

La organización gestiona la seguridad desde la perspectiva de gestión de riesgos. Los riesgos serán considerados desde todas las dimensiones afectas. Se mantendrán las tres dimensiones clásicas de seguridad, integrándose además las dimensiones referenciadas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad: confidencialidad, integridad y disponibilidad, así como dimensiones de autenticidad y trazabilidad. Se considerará la esfera de privacidad referenciada por la Autoridad de Control en su guía de referencia -*Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*-, con sus dos dimensiones derivadas de la probabilidad y gravedad variable para los derechos y libertades de las personas físicas. Se consideran por un lado los riesgos asociados a la protección de la información y por otro,

los riegos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados. La gestión de los riesgos permitirá una gestión de la seguridad del sistema de manera global e integral.

Para soportar esta política, se establecerán políticas de seguridad, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio. La presente Política será accesible para las partes internas y externas afectadas.

## 5.1. Principio de Seguridad

Se implanta una estrategia corporativa para garantizar la seguridad del sistema y de los servicios prestados, lo que implica necesariamente que todos los recursos deben disponer y aplicar las medidas mínimas de seguridad exigidas, y en concreto las que surjan del plan de tratamiento de riesgos y las que sean de aplicación de las contenidas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En consideración a la Disposición Adicional Primera de la LOPD, se considerará que el Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

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, como responsable o como encargado del tratamiento, la organización aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, considerando la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento –considerando la trazabilidad y autenticidad-; 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.

La dirección ha considerado emplear estándares de seguridad, para alinear los procesos y la seguridad del sistema, siendo la principal referencia el Real Decreto 311/2022, junto con otras normas de uso no obligatorias, pero de consideración, y específicamente la serie de Guías 800 publicadas por el Centro Criptológico Nacional CCN-CERT. Se han considerado normas de base como la ISO 31000 para el análisis de riesgos.

Todos los recursos deben disponer y aplicar aquellas medidas mínimas de seguridad exigidas, y en concreto las que sean de aplicación de las contenidas en el Anexo II Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en solitario o en conjunto con aquellos controles paralelos y de análoga naturaleza, derivados del análisis de riesgos.

La organización puede considerar la necesidad de someterse a una revisión de conformidad por un tercero que certifique el nivel de cumplimiento y adecuación de la organización a la normativa implicada. La dirección puede considerar certificaciones derivadas que afecten al sistema.

## 5.2. Alcance

La presente política, afecta a los datos personales gestionados y tratados por el grupo. Con independencia de que el presente manual aplique a todas las empresas del Grupo SEPIDES, cada una de ellas es responsable del tratamiento de sus propios datos.

Como gestores de datos, por disponer de su acceso y operar sobre los mismos, será aplicable a todo el personal propio y de terceros.

Todo el personal tiene la responsabilidad de garantizar el cumplimiento de los principios de la normativa de protección de datos y mantener el pleno cumplimiento de la presente política.

Quedan afectados todos los datos, con independencia de su sistema de tratamiento y del medio en que sean gestionados.

La organización ha considerado un sistema de gestión de registro de actividades de tratamiento, que a nivel corporativo permitirá gestionar de manera centralizada todo el proceso de tratamiento de datos. Todas las actividades de tratamiento están sometidas a la presente política. La matriz gestionará un registro de actividades valido para las entidades filiales. No obstante, las filiales que no requieran un registro de actividades podrán ser excluidas de los registros de operaciones definidos. La función de delegado de protección de datos será la de custodia del registro de actividades de tratamiento. Se designarán responsables funcionales o propietarios de cada registro, y deberá mantener actualizada a información del registro correspondiente, debiendo informar al menos, cada 6 meses al Delegado de Protección de Datos.

La organización trata categorías de datos diferenciadas, todas ellas sometidas a la normativa de privacidad.

A modo meramente indicativo y no exhaustivo, tratamos;

a) Datos identificativos. Como el nombre completo, el documento de identificación o carnet de conducir.

b) Datos de contacto. Como el teléfono o el correo electrónico.

c) Categorías de datos especiales. Como datos biométricos.

d) Datos de infracciones. Pero solo en determinados usuarios del sistema y bajo el estricto control.

e) Datos de formación. Como títulos o capacitaciones, certificados habilitantes y estudios en proceso.

f) Datos de profesionales. Relacionados con la experiencia profesional y empleos anteriores.

g) Otros datos. Por ejemplo, aquellos relacionados con evaluaciones de puestos, rendimiento profesional, números de cuenta bancaria, etc.

Nuestra organización trata datos de diferentes categorías de interesados. A modo enunciativo, especificamos que tratamos datos de:

a) Consejeros, empleados, personas en prácticas/formación y potenciales empleados.

b) Colaboradores y trabajadores de terceros con los que tenemos relación de prestación de servicios o acuerdos comerciales o de negocio.

c) Clientes y personas de contacto de clientes.

d) Personas de contacto de órganos y entidades públicas o privadas, así como cargos públicos.

## 5.3. Objetivos Generales

Son objetivos de la política de seguridad y de protección de datos:

- **Mantener el pleno cumplimiento legal**, alineando los procesos y los servicios, a la normativa vigente en cada momento, y muy especialmente al declarado en la normativa de Protección de datos y al Real Decreto 311/2022.
- **Mantener un sistema de gestión de seguridad**, conforme a los criterios establecidos en el RGPD y la LOPD y en el Real Decreto 311/2022, estructurando la gestión eficiente y eficaz de la seguridad de acuerdo a aquella y a las buenas prácticas del sector (incluyendo las Guías publicadas por el CCN-CERT). Se consideran las directrices del Comité Europeo de Protección de Datos y doctrina emanada de la(s) Autoridad(es) de Control y/ o Jurisprudencia, respecto a la seguridad de la información personal.
- **Establecer y difundir los roles y responsabilidades** relacionados con la Seguridad y la privacidad / protección de datos.
- **Sensibilizar y concienciar de manera estable y permanente al usuario** de la organización mediante el impulso de acciones por la dirección y la ejemplificación de la misma, en las tareas de seguridad más críticas.
- **Disponer de respuestas a los incidentes y brechas de seguridad**, mediante respuesta activa –reactiva y proactiva- y acciones preventivas y detectivas, y cuando fuera preciso acciones de respuesta y recuperación, adecuadas y detalladas, generando las comunicaciones y notificaciones pertinentes.
- **Asegurar que los activos de la organización**, sólo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- **Proteger** la información interna y la relacionada con la prestación de los servicios / clientes, considerando las dimensiones de:
    - Confidencialidad: Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.
    - Integridad: Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.

- Disponibilidad: La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.
- Trazabilidad: Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- Autenticidad: Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

## 5.4. Principios Generales de Protección de Datos

La organización requiere los datos personales para el pleno cumplimiento de sus fines.

Los datos se tratarán de manera lícita, leal, transparente, con fines determinados y explícitos, legítimos sin ser usados para fines posteriores incompatibles. Serán datos adecuados, pertinentes y limitados, exactos y actualizados. Serán tratados durante el tiempo necesario garantizándose la seguridad de los mismos. Para ello, se concretizan unos principios generales:

- La responsabilidad activa. Como responsables de los datos o encargados de acciones para un responsable de los datos, realizaremos las actuaciones pertinentes para mantener la seguridad de los datos. La organización ha considerado, la gestión de los datos empleando un sistema de registro de actividades de tratamiento, que permitirá evidenciar la conformidad legal de los tratamientos.
- Seguridad basada en el riesgo. Se aplicarán las medidas técnicas y organizativas apropiadas para garantizar y demostrar, que el tratamiento es conforme con la normativa de protección de datos y que las acciones sobre los datos no suponen un riesgo para las mismas.
- Los datos serán tratados de manera justa, leal y transparente. No se tratarán datos que no cumplan las condiciones de seguridad básicas. No se recogerán más datos de los necesarios y solo aquellos que sean requeridos para satisfacer la operativa de la organización y el negocio.
- Se asegurará la calidad de los datos personales y su precisión. De manera que se actualizarán o eliminarán cuando no estuvieran al día o fueran incompletos. La organización mantendrá controles adecuados para evitar que la información personal no sea exacta y para que se mantenga solo, durante el plazo de conservación estrictamente permitido.
- Se suspenderán los tratamientos que no reúnan las garantías de seguridad. Se podrá demostrar en todo momento que se mantienen las garantías de seguridad y las medidas técnicas y organizativas apropiadas para evitar el tratamiento no autorizado o ilegal de los datos personales y se protegerán los datos contra las pérdidas o destrucción accidental. Se desarrollarán los principios de protección de datos por defecto y en el diseño.
- No se realizarán envíos de información personal sin las medidas de seguridad adecuadas. Cualquier envío será realizado con una máxima seguridad y diligencia por parte de los usuarios del sistema.

- Existirá una persona o departamento o área específica, con responsabilidad específica y conocimiento en protección de datos personales. Será el contacto interno para otras áreas o departamentos o usuarios del sistema, y para contacto externos, tanto proveedores o colaboradores, como titulares de datos, que se encargará de asesorar, responder a consultas, cooperar con las áreas, ser un punto de contacto y unificación en la materia, gestionar los riesgos, y otras funciones específicas. Existirá un punto único a nivel de grupo que desarrollará estas funciones, pudiendo existir pequeñas unidades o personas de referencia en otras organizaciones, cuando a nivel de grupo se considere adecuado y pertinente.
- Se respetarán los derechos de los interesados y se tramitarán todas las solicitudes de ejercicio de derechos de un titular. La organización considerará cualquier solicitud de una persona física, y se tramitará siempre conforme al procedimiento establecido. Se tomarán medidas antes de divulgar cualquier información personal que se tenga, de conformidad con las disposiciones permisivas de la legislación o exención aplicable.
- Los usuarios con acceso a la información personal mantendrán un secreto constante y adoptarán medidas de seguridad pertinentes. Serán formados e informados de manera permanente y constante.
- Se generarán acciones de control para asegurar que los riesgos están siendo gestionados. Se generarán evaluaciones regularmente y cuando sea necesario. Cuando se detecten acciones de los usuarios que supongan infracciones de las normas y procedimientos establecidos y que supongan un riesgo a los datos personales, podrán dar lugar a acciones disciplinarias.
- Sensibilización. Concienciación. Formación. La organización declara la necesidad de formar, informar y sensibilizar a todos los usuarios con acceso a los datos personales. Para ello se considerarán diferentes niveles de sensibilización y formación en función del perfil de los usuarios, del acceso a los datos requeridos y de la categoría de datos y titulares de datos a los pudieran estar accediendo. Se considerará un plan de formación y de sensibilización para que en un ciclo completo de tres años se realicen diferentes acciones encaminadas a mejorar la seguridad de los datos.
- Cumplimiento. Los usuarios del sistema, son informados de la política de privacidad y de los principios consagrados en la misma y de la necesidad de cumplirla, debiendo lograr que sean plenamente conscientes, que el no cumplimiento de la misma puede acarrear medidas disciplinarias.
- Colaboración. Nuestra organización, nuestro Delegado de Protección de Datos, nuestros usuarios, y nuestros proveedores deben colaborar con el cumplimiento de la presente política y específicamente, colaborarán con la autoridad de control, cuando la misma evalúe el cumplimiento de la normativa de privacidad.

## 5.5. Principios Particulares de Protección de Datos

**Legalidad**

a) Todos los datos tratados por la organización deben tener una de las siguientes bases de licitud: consentimiento, contrato, obligación legal, intereses vitales, interés público o intereses legítimos.

b) La organización deberá indicar la base de licitud apropiada en el Registro de actividades.

c) Cuando se establezca el consentimiento como base de licitud, se conservará la evidencia del consentimiento suficientemente válida para acreditar el cumplimiento.

d) Cuando se envíen comunicaciones o Newsletter, en función de su consentimiento, la opción para que el individuo revoque su consentimiento debe estar claramente disponible y deben existir sistemas para garantizar que dicha revocación sea efectiva.

**Minimización**

La organización se asegurará que los datos personales sean adecuados, relevantes y estén limitados a lo que sea necesario en relación con los fines para los que se procesan.

**Exactitud**

La organización adoptará medidas razonables para garantizar que los datos personales sean precisos, exactos y estén actualizados.

Cuando sea necesario para la base de licitud, se deberán implementar los pasos necesarios para garantizar que los datos personales se mantengan actualizados.

La inexactitud de los datos no será imputable al responsable del tratamiento, siempre que hayamos adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se los tratamos, cuando los datos sean inexactos o se tengan sospechas de ello.

**Conservación**

Para garantizar que los datos personales no se conserven o traten durante más de lo necesario, la organización establecerá un procedimiento de calificación de la información que regula el proceso de archivo.

La política de calificación de la información declarará la información personal que debe conservarse, por cuánto tiempo y para que finalidad.

**Responsabilidad proactiva**

La organización será capaz de demostrar el cumplimiento de la normativa de protección de datos, y específicamente de los principios y de la seguridad de los datos.

La organización demostrará el cumplimiento de los principios de protección de datos mediante la aplicación de políticas de protección, adhiriéndose a los códigos de conducta cuando sea necesario, la implementación de medidas técnicas y organizativas, así como la adopción de medidas tales como protección de datos por

diseño, Evaluación de Impacto, notificación de incumplimiento procedimientos y planes de respuesta a incidentes.

**Confidencialidad**

Como Responsable y como Encargado, seremos responsables de que todos los usuarios que intervengan en las operaciones sobre los datos, se sometan a la estricta confidencialidad, siendo esta obligación complementaria de los deberes de secreto profesional que pudieran existir de conformidad con otras normativas aplicables.

La obligación de secreto se mantendrá de manera indefinida.

**Seguridad**

La organización debe asegurar de que los datos personales se almacenen de forma segura. Se extremarán las medidas de seguridad y se mantendrán a nivel operativo todas las actualizaciones y mejoras requeridas para mantener el software actualizado.

El acceso a los datos personales se limitará al personal que necesite el acceso. Existirá seguridad adecuada para evitar el intercambio o acceso no autorizado a la información personal.

La eliminación de los datos personales se hará de forma segura, y siempre de manera que los datos sean irrecuperables.

Se deben implementar soluciones apropiadas de respaldo y recuperación ante desastres.

## 5.6. Gestión Documental de la Seguridad

La seguridad del sistema de información se documentará mediante procedimientos y procesos de operación que serán puestos a disposición de los usuarios implicados en el mismo.

Los cambios serán gestionados, las capacidades del sistema serán medidas y controladas y los entornos estarán separados.

Se documentarán los acuerdos con proveedores y colaboradores formando parte del sistema.

La cadena de suministro será controlada en relación a los requisitos de seguridad, la prestación de servicios o los cambios de suministradores, no permitiéndose el acceso a datos personales o al sistema a proveedores que no garanticen la seguridad de la información y de los datos personales.

Se desarrollarán procedimientos de protección del sistema, incluyendo procedimientos de copias y restauración, y cuantas vulnerabilidades pudiera tener el sistema.

Las comunicaciones serán gestionadas, desde entornos de redes a intercambios operativos incluidos en los procesos. Se incluirá cuando sea necesario, el cifrado o el control de comunicaciones de mensajería instantánea.

Para soportar esta política, se establecerán otras políticas, normas y procedimientos detallados, los cuales serán publicados y comunicados a todos los usuarios, terceros y socios de negocio.

## 5.7. Gestión del Riesgo

La gestión de riesgos se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema de información y la organización, basándose en la Metodología reconocida en el sector, que en todo caso será metodología detallada y documentada, que permitirá la repetición de la medición y análisis, a intervalos planificados, al menos una vez al año salvo que no hubiera modificaciones, y cada vez que el sistema tenga cambios sustanciales.

Es obligación de la entidad, la ejecución de las evaluaciones de impacto que sean precisas de conformidad con la normativa de protección de datos.

La gestión de riesgos permitirá el mantenimiento de un entorno de seguridad controlado, minimizando los riesgos hasta niveles aceptables para la dirección. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de la información, los riesgos a los que estén expuestos, los derechos y libertades de las personas físicas y las medidas de seguridad.

La organización evalúa el nivel de riesgo para las personas asociado con el tratamiento de sus datos personales. Cuando sea necesario desarrollaremos, conforme a los procesos establecidos por la Autoridad de Control, las Evaluaciones de Impacto –PIA / DPIA- en relación con el tratamiento de los datos.

Cuando un tipo de tratamiento, en particular utilizando nuevas tecnologías y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, sea probable que resulte en un alto riesgo para los derechos y libertades de personas físicas adoptaremos antes del tratamiento las medidas precisas para salvaguardar los datos.

## 5.8. Gestión de Incidencias de Seguridad

El proceso de gestión de incidentes, incluirá la detección y notificación de las incidencias, los criterios de clasificación, los procedimientos de análisis y resolución, así los cauces de comunicación a las partes interesadas –especialmente cuando afecta a terceros- y el registro de las actuaciones ejecutadas.

Cuando estas evidencias afecten a datos personales, deberá contarse con el Delegado de Protección de Datos –cuando estuviera designado-. Las violaciones de seguridad que generen riesgos de divulgación, pérdida, destrucción o alteración, serán gestionadas por el Delegado. Se considerarán los requerimientos del procedimiento desarrollado al efecto, para comunicar y notificar las mismas a las autoridades de control y a los usuarios afectados.

No obstante, se establece que las violaciones de seguridad serán notificadas al Responsable de Seguridad que colaborara en todo lo necesario con el Delegado.

## 5.9. Gestión de los Derechos de los Interesados

La organización respetará los derechos de los interesados y facilitará información respecto a los mismos.

En concreto, se considerará;

- Derecho a obtener una copia de la información que comprenda los datos personales, sin coste dentro del plazo de un mes desde la solicitud del interesado,
- Derecho a rectificar los datos inexactos o incompletos datos personales,
- Derecho al borrado de los datos personales cuando ya no sean necesarios, si los datos han sido procesados ilícitamente o si el interesado se retira su consentimiento, salvo que haya un interés legal o público primordial en continuar tratando los datos,
- Derecho a limitar el tratamiento de sus datos personales mientras se tramitan procesos al respecto del tratamiento o una reclamación legal al respecto.
- Derecho a la portabilidad de datos; cuando el tratamiento se base en el consentimiento o en un contrato y el procesamiento sea automatizado.
- Derecho a objetar y evitar el tratamiento posterior de los datos para el Intereses legítimos o interés público.
- Derecho a que no se traten los datos para mercadotecnia directa.
- Derecho a no verse sometido o a presentar objeciones respecto a las decisiones individuales.
- Derecho a reclamar indemnización por los daños causados por un uso poco diligente de los datos personales.

## 5.10. Gestión de las Transferencias de Datos a Terceros Países u Organizaciones Internacionales

Todas las exportaciones de datos que desde el Espacio Económico Europeo (EEE) realicemos a países no europeos, se considerarán a todos los efectos transferencias a terceros países, y serán consideradas como no válidas salvo que, haya un "nivel de protección apropiado para los derechos fundamentales de los titulares de datos".

Como organización declaramos la necesidad de disponer de un principio de seguridad para la transferencia de datos fuera del Espacio Económico Europeo. Adoptaremos las cláusulas contractuales establecidas por la Unión Europea y recabaremos la Autorización de la Autoridad de Control cuando corresponda.

La organización declara la prohibición de la transferencia de datos personales fuera del EEE a menos que al menos se cumpla una de las salvaguardas requeridas, o excepciones aplicables:

**Una decisión de adecuación**

Se trate de un país evaluado por la Comisión Europea en el que existe un nivel apropiado de protección de los derechos y libertades de las personas En estos casos, no se exigirá autorización expresa de la autoridad de control.

A estos efectos se consideran países que son miembros del Espacio Económico Europeo (EEE) pero que cumplen las condiciones para una adecuación, por constar publicados en el Diario Oficial de la Unión Europea, los incluidos en la siguiente lista;

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

**Otros supuestos**

Cuando no nos encontremos en los supuestos previos, deberemos considerar los siguientes supuestos;

a) Consentimiento del interesado previa información, para realizar la transferencia.

b) La transferencia es necesaria para la ejecución o conclusión de un contrato.

c) La transferencia es necesaria para el establecimiento, ejercicio o defensa de intereses.

d) La transferencia es necesaria para proteger los intereses vitales.

Fuera de estos supuestos, queda totalmente prohibido realizar una transferencia a un estado fuera del Espacio Económico Europeo.

## 5.11. Gestión de las Revisiones

Se realizará una verificación, evaluación y valoración anual, o cada vez que haya cambios significativos en los tratamientos de datos, de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Las revisiones serán realizadas por la dirección tras los correspondientes reportes periódicos.

Existirán revisiones internas o auditorías del sistema desarrollados por áreas o departamentos específicos. El delegado de protección de datos, revisará el nivel de cumplimiento de protección de datos y los incumplimientos derivados. El delegado informara periódicamente a la dirección.

Específicamente la entidad y el sistema se podrán someter a procesos de certificación externos. La entidad puede considerar someter el sistema a los mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD, en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de la entidad, considerada en toda su magnitud y con todas las filiales, y todo ello de conformidad con el artículo 42 del RGPD.

La dirección podrá adherirse a códigos y otros estándares de seguridad que permitan adecuar el tratamiento de la información personal a los principios declarados.

## 5.12. Aprobación

La presente política será aprobada por el consejo de administración, asumiendo el compromiso de proveer todos los recursos y medios para la implementación de las medidas de seguridad necesarias para mantener la seguridad, integridad, disponibilidad y resiliencia del sistema, así como la trazabilidad y autenticidad.

La dirección establece la necesidad de cumplir con la presente Política, así como el resto de Políticas, Procedimientos, Instrucciones y Normas desarrolladas al efecto y de velar por su cumplimiento, y a tales efectos aprueba y publica esta política para su correcta difusión.

# 6. TRATAMIENTOS ORGANIZADOS: REGISTRO DE ACTIVIDADES. PRINCIPIOS

## 6.1. Objeto

En el marco del sistema desarrollado en el GRUPO SEPIDES, en materia de protección de datos, se llevará un registro de actividades de tratamiento, que se realice en cada entidad responsable.

Con independencia de que el presente manual aplique a todas las empresas del Grupo SEPIDES, cada una de ellas es responsable del tratamiento de sus propios datos y por tanto desarrollará los correspondientes registros cuando sea necesario y será custodio de los mismos.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el Reglamento.

Cuando se considere pertinente, se gestionará un solo registro de actividades común a todas las sociedades que será custodiado por el Delegado de Protección de Datos.

## 6.2. Registro de Actividades

Para demostrar la conformidad con la normativa vigente en materia de datos personales, bien como responsable o bien como encargado del tratamiento deberemos mantener registros de las actividades de tratamiento bajo nuestra responsabilidad.

Dispondremos de un inventario de datos y del flujo de datos como parte del enfoque de seguridad del tratamiento de datos y para abordar los riesgos y oportunidades.

En nuestro registro de actividades, se podrá identificar, los procesos en los que se usan datos personales; las fuentes de datos personales; el volumen de sujetos de datos; la descripción de la categoría de datos personales; actividades de procesamiento; los fines para los que se utiliza cada categoría de datos personales; los destinatarios de los datos personales; cualquier transferencia de datos; y todos los requisitos de retención y eliminación.

## 6.3. Tipos de Registros de Actividades

**A.-Como Responsable**

Llevaremos un registro de las actividades de tratamiento efectuadas bajo nuestra responsabilidad, y que contendrá al menos, la información que requiere la normativa de protección de datos, y específicamente, la identificación del delegado de protección de datos, los fines, categoría de los interesados y de los datos personales, categoría de destinatarios de cesiones, y en su caso, las transferencias internacionales.

**B.- Cuando seamos Encargados de Tratamiento**

Llevaremos un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, con el contenido requerido por la normativa.

Cuando la organización disponga de encargados de tratamiento, les requerirá el correspondiente registro implicado en el servicio concertado.

## 6.4. Principios Implicados en el Registros de Actividades

Con carácter general;

- Nuestras fichas de tratamiento permitirán cumplir el principio de transparencia, ofreciendo toda la información relativa al tratamiento de datos, de manera accesible y fácil de entender.
- En nuestro registro de actividades se declarará la identidad que como responsable del tratamiento tenemos – *o como encargado, la de nuestros responsables-.*
- Se identificarán claramente los fines del mismo y la información que nos permita garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas.
- Como responsable y como encargado, estamos obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, nuestras fichas de registro, de modo que puedan servir para supervisar todas nuestras operaciones de tratamiento.
- 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. Para ello, declararemos los plazos en nuestras fichas de registro de actividades como Responsable.
- El Registro de Actividades deberá constar siempre por escrito documentándose las modificaciones realizadas en los mismos identificando la fecha y el responsable de la citada actualización.

## 6.5. Roles y Responsabilidades en el Registros de Actividades

Se considera quién debe actualizar y quien realizar trámites operativos en relación con los Registros de actividades.

El delegado de protección de datos custodiará los Registros e informará de su necesidad de actualización. El Delegado de Protección de Datos será quien asesora o quien informa, repartiendo las tareas con los responsables funcionales o propietarios de los registros.

Responsable de cada Registro de Actividades será el área o departamento asignado, que se considerará como responsable funcional o propietario de la actividad de tratamiento.

Se consultará al delegado de protección de datos cuantas dudas se tuvieran en relación a los registros de los que se pudiera ser responsable.

## 6.6. Procedimientos sobre Registros de Actividades

**Creación de un Registro de actividades**

1. Detectada una nueva operación/operaciones de tratamiento de datos personales por parte de un responsable funcional o un propietario, lo comunicará al Delegado de Protección de Datos incluyendo los siguientes puntos:
   - Denominación de la operación o conjunto de operaciones.
   - Finalidad.
   - Base de licitud.
   - Categoría de interesados afectados y de datos tratados.
   - Medidas técnicas y organizativas propuestas por el área.
2. Recibida la comunicación, el delegado de protección de datos valorará la creación de una nueva actividad o bien la inclusión en una ya existente, comunicando la decisión al área- El DPD podrá pedir asesoramiento del responsable de seguridad para valorar las medidas técnicas propuestas en la nueva actividad.
3. El área en caso de desacuerdo podrá presentar las alegaciones que considere pertinentes si considera que la petición debe ser atendida. El DPD emitirá opinión al respecto una vez sean valoradas las alegaciones presentadas.
4. En todo caso, esta propuesta debe realizarse antes de que se lleve a cabo una nueva actividad de tratamiento de los datos personales, debiendo además tenerse en cuenta la necesidad de adaptar otras medidas, atendiendo al principio de privacidad desde el diseño, como pueden ser el análisis de riesgos de la nueva actividad o, en su caso, una evaluación de impacto.

**Modificación del Registro**

1. Cada área revisará periódicamente la vigencia del contenido de las actividades de tratamiento bajo su responsabilidad, valorando la necesidad de actualizar o modificar las mismas.
2. Deberá quedar constancia escrita de la fecha de actualización, motivo de la misma y persona encargada de su ejecución. Podrá recabar el asesoramiento del responsable de seguridad cuando las medidas técnicas del tratamiento puedan verse afectadas.
3. Las modificaciones realizadas deberán ser comunicadas al Delegado de Protección de Datos Personales por escrito y en el plazo de 72 horas desde su realización.

**Supresión**

1. Si se detectase que una actividad ya no se está prestando, tanto cuando la organización actúa como responsable como de encargado, deberá comunicar por escrito la situación al Delegado de Protección de Datos.
2. El Delegado de Protección de Datos valorará la petición de supresión e informará al área sobre su decisión. Podrá considerar el asesoramiento del responsable de seguridad.

3. El responsable de la tarea procederá, en su caso, a la supresión de la actividad del Registro, procediendo, una vez efectuada, a comunicarlo al Delegado de Protección de Datos Personales.

## 6.7. Publicidad de Registros de Actividades

Las modificaciones relacionadas con el Registro de Actividades deben ser comunicadas al Delegado de Protección de Datos, que es el encargado de poner a disposición de la autoridad de control (AEPD) los documentos contenidos en el Registro de Actividades del tratamiento si así le fuese requerido por la misma.

El Delegado de Protección de Datos será el custodio del Registro y controlará las versiones, según los cambios efectuados por cada propietario o responsable funcional.

El Delegado de Protección de Datos mantendrá permanentemente actualizado el fichero documental del Registro de Actividades, pudiendo requerir documentación al resto de los responsables implicados en la gestión, que deberán responder diligentemente y en el menor plazo posible.

El Delegado podrá auditar periódicamente el contenido del Registro, la vigencia de su contenido y la eficacia de las medidas de seguridad técnicas y organizativas referenciadas con el asesoramiento del responsable de seguridad.

De conformidad con las previsiones establecidas en la normativa vigente, el Delegado de Protección de Datos podrá recomendar la publicación del inventario de Actividades.

# 7. POLÍTICA DE PRIVACIDAD POR DISEÑO Y POR DEFECTO

## 7.1. Objeto

En el marco del sistema desarrollado en el GRUPO SEPIDES, en materia de protección de datos, los principios de privacidad por diseño y privacidad por defecto significan que, para cada proyecto, debemos implementar de manera proactiva e implementar sólidas prácticas de protección de la privacidad. La seguridad se entenderá como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

## 7.2. Privacidad por Diseño

La aplicación del principio de privacidad por diseño con respecto a un Proyecto de Tratamiento de Datos Personales significa que la protección de la privacidad y el cumplimiento de la normativa de Protección de Datos se convierten en un elemento clave y una prioridad dentro del proceso de diseño y gestión del Proyecto, en la etapa más temprana posible del Proyecto y durante todo su ciclo de vida.

El interesado no debe desarrollar medidas de seguridad sobre sus datos. Cuando se requiera el tratamiento de los datos de los interesados en nuestros proyectos y servicios, se establecerán medidas por defecto para garantizar la seguridad de los datos. En concreto procuraremos el pleno cumplimiento del principio de Protección de Datos por diseño y por defecto (artículo 25 del RGPD), Seguridad en el tratamiento (artículo 32 del RGPD), Evaluaciones de Impacto (artículo 35 del RGPD) y funciones del Delegado de Protección de Datos (artículo 39 del RGPD).

Se considera un Proyecto de Protección de Datos, cualquier sistema de información gestionado desde o por el grupo, así como los subsistemas que pudieran estar integrados.

El Delegado de Protección de Datos, deber ser incluido siempre en la etapa más temprana del diseño y desarrollo de sistemas de información, cambios en la arquitectura o infraestructura, desarrollo de aplicaciones o herramientas, o líneas de negocio-actividades.

## 7.3. ¿Qué Significa Privacidad por Diseño?

Debemos integrar plenamente en el diseño del proyecto (y la gestión del proyecto) todas las medidas necesarias para proteger la privacidad y los Datos Personales.

El orden de prioridades que hemos aplicado hasta ahora se invierte. La protección de la privacidad y los Datos Personales y el cumplimiento de la normativa de protección de Datos ya no son consideraciones en las que pensamos al final de toda la configuración del proyecto. Ahora, implementar todas las medidas técnicas y organizativas para garantizar la protección de la privacidad y el cumplimiento de la normativa de protección de Datos es un factor clave que debe integrarse en la gestión del proyecto de principio a fin.

Adoptar un enfoque de privacidad por diseño implica incorporar todas las medidas técnicas y organizativas posibles en el Proyecto para implementar los principios de privacidad y protección de Datos, como la minimización de Datos. Un ejemplo de medida técnica es la seudonimización sistemática de los Datos Personales que se recopilan, que es una medida que hace menos probable identificar a un individuo cuando no es necesario.

Al aplicar el principio de privacidad por diseño, tomaremos en cuenta el estado de la técnica, el coste de la implementación de medidas técnicas y organizativas, la naturaleza, el alcance, el contexto y las finalidades de un Tratamiento, así como los riesgos de los derechos y libertades de los Titulares de los Datos planteados por el Tratamiento.

Para mantener el proceso de seguridad integral, se realizará una clasificación de la información-, conforme a los principios de protección frente a pérdidas, accesos indebidos, divulgación o uso indebido, deterioro de la información o pérdida de disponibilidad. La clasificación conllevará necesariamente una política de etiquetado y manipulación. La información personal estará integrada en el sistema y será categorizada. Para mantener el proceso de seguridad integral, se realizará una gestión de los activos.

Se deberá conocer en todo momento el estado de seguridad del sistema o de sus componentes, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les puedan afectar.

## 7.4. Privacidad por Defecto

También debemos tener siempre una actitud de privacidad y enfoque predeterminados al implementar actividades de Tratamiento en el marco de los proyectos de GRUPO SEPIDES.

Las funciones de operación, administración y registro de actividad, serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde localizaciones o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso.

El uso del sistema será sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Se incorporará la privacidad y protección de datos en los sistemas a lo largo del ciclo de vida de los datos: “recolección-uso-divulgación-retención-destrucción”.

Se incorporarán a los proveedores en los requisitos de seguridad por defecto que dispongamos.

## 7.5. ¿Qué Significa Privacidad por Defecto?

Con las medidas de “privacidad por defecto”, lo que se pretende es que Grupo SEPIDES, por defecto, el tratamiento de los datos personales sea siempre, bajo los estrictos controles de seguridad.

La privacidad por defecto se aplica a los siguientes aspectos:

- Cuántos Datos Personales estamos recolectando,
- Qué queremos hacer exactamente con estos Datos Personales,
- Cuánto tiempo queremos conservar estos Datos Personales, y
- Quién tendrá acceso a estos Datos Personales.
- Como se dispone el tratamiento y el conjunto de operaciones sobre los datos.

Al decidir qué Datos Personales recopilar o usar para un Proyecto específico, debemos preguntarnos si no es posible implementar ese Proyecto con menos Datos Personales;

Cuando decidamos durante cuánto tiempo debemos conservar un determinado conjunto de Datos Personales que GRUPO SEPIDES recopila y utiliza, siempre debemos elegir el período más breve posible en función del objetivo del Tratamiento. La organización dispondrá de unos plazos de conservación asociada a una política de calificación.

Los accesos a los datos serán analizados previamente. Solo los usuarios que requieran para el ejercicio de sus funciones el acceso a los datos, podrán acceder.

Impacto de los principios de la privacidad por diseño y privacidad por defecto en la gestión, descripción y aprobación del Proyecto.

Para cada proyecto, debemos ser capaces de demostrar que cumplimos con los principios de privacidad por diseño y privacidad por defecto, y cómo se han integrado estos principios a la gestión del proyecto.

Los controles de privacidad deben integrarse en la arquitectura de los sistemas de TI, las operaciones y los procesos de negocios sin disminuir la funcionalidad del usuario.

## 7.6. El Delegado de Protección de Datos es Responsable de:

En cualquier proceso o proyecto de nuevo desarrollo o en fase de revisión/ modificación, se involucrará al Delegado de Protección de datos, a fin de que este pueda establecer pautas de privacidad desde el diseño y por defecto.

Se considerará cuando así lo determine el Delegado, involucrar a responsables y empleados con respecto a las actividades de Tratamiento impactadas, en el momento del proceso de toma de decisiones y el diseño del Proyecto subyacente.

Se documentará y mantendrán registros y evidencias de la integración de los principios de privacidad por diseño y por defecto en el proceso de gestión del proyecto.

Se considerarán los siguientes puntos a desarrollar para mantener la privacidad desde el diseño y por defecto.

1. **Protección Preventiva y Proactiva**

   Todos proyectos y servicios, estarán concebidos y diseñados considerando los riesgos a la privacidad. Cualquier producto implicado en el servicio, y específicamente software necesario para el desarrollo de los proyectos o servicios, serán analizados desde la perspectiva de privacidad.

   A mayor abundamiento, las aplicaciones dispondrán de evidencias de cumplimiento de los requerimientos de seguridad incluidas, certificaciones, y podrán ser auditadas a efectos de la privacidad.

2. **Privacidad "por Defecto"**

   El personal, tendrá accesos a los sistemas con una configuración por defecto, y esta será la más segura posible en términos de protección de los datos personales. No se deben recoger, almacenar ni tratar datos personales, salvo que sea imprescindible para la finalidad perseguida.

3. **Privacidad integrada en el Diseño**

   El servicio a desarrollar en todas sus fases, integrara como elemento central la protección de los datos personales, generando la misma importancia que la

propia funcionalidad. En consecuencia, se desarrollará cuando sea preciso revisiones, propias o de terceros, y desarrollará evaluaciones de impacto tanto a sus procesos y desarrollos como aquellos en los que intervenga un tercero implicado en el servicio.

Las evaluaciones de impacto se desarrollarán en el diseño e inicio de nuevos servicios, como mecanismos de análisis de los riesgos potenciales y elaboración de medidas de tratamiento adecuadas.

4. **Funcionalidad Plena**

   El proyecto o servicio será diseñado y se desarrollará en sus fases iniciales, pero también en su funcionalidad o desarrollo avanzado y en cualquier fase, siguiendo la premisa de eficacia y funcionalidad, con el máximo respeto privacidad.

5. **Protección durante todo el Ciclo de Vida**

   La privacidad integrara todo el proceso y el servicio desde el diseño y será un estándar durante la ejecución de los servicios, de manera que se desarrollaran como medidas preferentes durante los servicios, la seudoniminzación y la encriptación-siguiendo los estándares adecuados, la custodia de las claves, la autenticación segura y la no generación de datos no cifrados-.

6. **Visibilidad y Transparencia:**

   Las políticas de seguridad, las medidas desarrolladas y los protocolos que los usuarios deben desarrollar en el proyecto están entregados a cada usuario afectado y se mantendrán a su disposición como mecanismo de refuerzo.

   Los usuarios disponen de un responsable de proyecto que podrá resolver cualquier duda relativa a la seguridad de los datos y a la funcionalidad del servicio. En su defecto consideraran la consulta o asesoramiento del Delegado de Protección de Datos.

7. **Respeto del Usuario.**

   El usuario final del sistema dispone de información valiosa sobre los principales riesgos que pueden materializarse. Además, se considerarán acciones de sensibilización y formación para dotar al personal de recursos adecuados para mantener la seguridad de los datos.

## 8. PROCEDIMIENTO DE GESTIÓN DE TERCEROS

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante RGPD, tiene un impacto significativo en el sistema desarrollado en el GRUPO SEPIDES, desde el propio Consejo de Administración, pasando por los departamentos y áreas y, aquellos terceros que pueden llegar a intervenir en nuestro sistema. El procedimiento de gestión de terceros está definido en el **Procedimiento de Gestión de Servicios Externos** del Sistema de Gestión de Seguridad de la Información.

# 9. PROCEDIMIENTO DE EJERCICIO DE DERECHOS DE LOS INTERESADOS

## 9.1. Objeto

Definir y normalizar un procedimiento que permita ejercitar los derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad por parte de las personas de la que se dispongan datos en el sistema, de acuerdo con el RGPD y la LOPD.

## 9.2. Responsabilidades

- El Delegado de Protección de Datos será responsable de:
  - Controlar la aplicación del presente procedimiento, garantizando los derechos de los afectados.
  - Controlar la existencia de vías de comunicación que permitan ejercitar los derechos aludidos.
  - Controlar la existencia del registro correspondiente a la persona que ejerce sus derechos, y que se cancelan, se modifican o se proporcionan dichos datos a la misma en los plazos legales establecidos.
- El Delegado de Protección de Datos será responsable de:
  - Verificar el cumplimiento de la consulta, baja, actualización, limitación o portabilidad de todos los registros existentes en cualquier sistema de información que se vean afectados por el mismo.

## 9.3. Desarrollo

En el marco del sistema desarrollado en el GRUPO SEPIDES, se garantiza el ejercicio de sus derechos a todas las personas físicas de las que trata datos, habilitando los cauces legales establecidos.

Cualquier usuario de la organización que reciba, ya sea verbalmente o por escrito, una solicitud por parte de un afectado deberá comunicárselo al GRUPO SEPIDES (DPD o Delegado de Protección de Datos, en su caso,) quien procederá, una vez analizada la petición, a facilitar al afectado el ejercicio de sus derechos, según proceda, en el plazo máximo de un mes, desde la recepción de la solicitud formal por parte del interesado.

El Delegado de Protección de Datos podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación de plazo al afectado dentro del primer mes.

Asimismo, si GRUPO SEPIDES decide no atender una solicitud, deberá informar de ello al afectado, motivando su negativa, dentro del plazo de un mes desde la presentación de solicitud de ejercicio.

GRUPO SEPIDES verificará la identidad de quienes soliciten acceso y de quienes ejerzan los restantes derechos reconocidos por el RGPD y la LOPD.

En los casos en que GRUPO SEPIDES trate una gran cantidad de información sobre un interesado podrá pedir a éste que especifique la información a la que se refiere su solicitud de ejercicio.

El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas. Así, GRUPO SEPIDES podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar (el canon no podrá implicar un ingreso adicional para GRUPO SEPIDES, sino que deberá corresponderse efectivamente con el verdadero coste de la tramitación de la solicitud).

## 9.4. Descripción

El afectado que ejercite alguno de sus derechos puede realizarlo de varias maneras:

1. **Presentación del afectado** en las instalaciones de GRUPO SEPIDES. En este caso, se debe de solicitar al afectado que ejerza su derecho por escrito, rellenando el formulario creado a tal efecto y exhibiendo documento identificativo (DNI, Pasaporte, Carné de Conducir, etc.). Se especificará la fecha de entrada del escrito para tener en cuenta a partir de qué momento comienza a contar el plazo para la contestación a la solicitud.

2. **Envío por correo postal** a la dirección de GRUPO SEPIDES o **por correo electrónico** a protecciondedatossepides@sepides.es

3. **Presentación a través de representante legal o voluntario acreditado**. Siguiendo los criterios de la Agencia Española de Protección de Datos, el ejercicio de los derechos por representante podrá dar sólo en dos casos:

    - Cuando el afectado sea incapaz o menor de edad,

    - Cuando haya otorgado un poder específico para ejercer un derecho concreto ante el tratamiento, para cada ocasión. Este poder debe haberse realizado en escritura pública, poder notarial o por cualquier otro medio reconocido en derecho.

Cuando SEPIDES tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud de ejercicio de derechos podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad de la persona afectada.

En aquellos casos en los que SEPIDES no haya solicitado la identidad al reclamante para el tratamiento de sus datos, -*por ejemplo, en el caso del tratamiento de datos para la remisión de newsletter, en la que solamente se solicita el correo electrónico*-, no se requerirá acreditación adicional para el ejercicio de derechos, sino la comprobación de los datos requeridos para llevar a cabo el tratamiento -por ejemplo, correo electrónico- y que figuran en los registros.

Una vez recibida la solicitud de ejercicio de derecho se enviará al Delegado de Protección de Datos de GRUPO SEPIDES quién procederá a examinar la solicitud para comprobar que reúne todos los requisitos, en concreto:

- **Titularidad del tratamiento de datos:** se comprobará que efectivamente se trata de una solicitud relacionada con los tratamientos de GRUPO SEPIDES. De este modo, en el supuesto de que el tratamiento de datos solicitados no esté

relacionado con el GRUPO SEPIDES, se responderá en este sentido, indicando que los únicos tratamientos sobre los que puede facilitar el ejercicio de derechos son aquellos sobre los que ostenta la titularidad.

- **Nombre, apellidos y firma del solicitante:** se comprobará que son los mismos que los que figuran en el documento identificativo que aporta el afectado. En caso de que en la solicitud no se aporte documento identificativo correspondiente o que la firma de la solicitud no se asemeje a la del documento identificativo, directamente se desestimará la solicitud por defecto de forma y se abrirá un periodo de subsanación. En estos casos se enviará una carta al afectado para solicitarle que proceda al envío de la documentación que falta.
- **Representación:** se comprobará que la persona que intenta ejercer el derecho tiene poder suficiente pare ello.

En colaboración con el responsable del departamento correspondiente el DPD procederá a ejecutar la operación solicitada:

- **Acceso:** Si la solicitud es de acceso y procede, se comunicará la información solicitada a la persona, incluida una copia de los datos personales objeto de tratamiento, por la vía elegida por la misma, en el plazo de un mes a contar desde la recepción de la solicitud.
- **Supresión:** Si la solicitud es de supresión y procede, se realizará la baja física del registro correspondiente y de todos aquellos sistemas donde figure dicha persona, sin perjuicio del deber de bloqueo en el plazo de un mes a contar desde la recepción de la solicitud.
  - La supresión de los datos podrá tener lugar cuando el dato sea erróneo, inexacto, lo solicite el interesado, no esté justificada la inclusión de dicho dato en el fichero o se encuentre en el fichero una vez transcurrido el plazo establecido para ello.
  - La supresión no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales, entre la persona o entidad responsable del tratamiento y el interesado, que justificaron el tratamiento de los datos.
  - Podrá también denegarse los derechos de rectificación o supresión en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa, o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
  - En caso de que no proceda la supresión por alguno de los motivos anteriormente expuestos, se deberá informar de ello al interesado expresando, además, la fecha en la que se procederá a la efectiva cancelación de los datos.
  - En todo caso, GRUPO SEPIDES informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas.

- **Rectificación:** Si la solicitud es de rectificación y procede, se realizará la modificación del dato correspondiente en todos y cada uno de los sistemas donde figure el mismo, y se enviará al solicitante la confirmación de la operación en el plazo de un mes a contar desde la recepción de la solicitud.

- **Oposición:** Si la solicitud es de oposición y procede, se cesará en el tratamiento de los datos de dicha persona en el plazo de un mes a contar desde la recepción de la solicitud. La oposición supone el cese en el tratamiento de los datos del afectado en los siguientes supuestos:

  - Cuando, por motivos relacionados con su situación particular, los datos personales que le conciernan sean objeto de un tratamiento basado en:

    - Una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
    - En la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero.

    En este caso, el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

  - Cuando se trate de tratamientos que tengan por finalidad la realización de actividades de publicidad, prospección comercial y elaboración de perfiles.

  - Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, salvo que dicha decisión se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado.

- **Portabilidad:** Si la solicitud es de portabilidad deberá proporcionarse en el plazo de un mes una copia de sus datos al interesado, que debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Este derecho sólo puede ejercerse:

  - Cuando el tratamiento se efectúe por medios automatizados.

  - Cuando el tratamiento se base en el consentimiento o en un contrato.

  - Cuando el interesado lo solicita respecto a los datos que haya proporcionado al GRUPO SEPIDES y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

  Los datos personales del interesado se transmitirán directamente desde el GRUPO SEPIDES a otra empresa que solicite el interesado, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible. Lo anterior no será aplicable:

  - A los datos de terceras personas que un interesado haya facilitado a un responsable.

- En caso de que el interesado haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable por terceros.

- **Limitación al tratamiento:** Si la solicitud es de limitación al tratamiento, en el plazo de un mes no se aplicarán a sus datos personales las operaciones de tratamiento que correspondan. Sólo se puede solicitar la limitación al tratamiento cuando:

  - El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud.

  - El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello.

  - Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

  - En el tiempo que dure la limitación, GRUPO SEPIDES sólo podrá tratar los datos afectados, más allá de su conservación:

    - Con el consentimiento del interesado.
    - Para la formulación, el ejercicio o la defensa de reclamaciones.
    - Para proteger los derechos de otra persona física o jurídica.
    - Por razones de interés público importante de la Unión o del Estado miembro correspondiente.

## 9.5. Contestación

Formulada la solicitud, resulta obligatorio contestar al afectado dentro del plazo legal, salvo en los casos en los que no se haya podido obtener una dirección donde realizar la correspondiente comunicación. La contestación se formulará en alguno de los siguientes términos:

- Si los datos que se encuentran contenidos en la solicitud no fueran suficientes, o se tratase de un solicitante diferente del afectado representante legal o voluntario, se requeriría al solicitante que los subsane.

- Si no se hubieran encontrado datos relativos a dicho solicitante, deberá comunicarse este hecho al afectado en el domicilio que figura en la solicitud.

- Si se hubieran encontrado datos, se contestará al afectado adjuntando los datos que de él se contienen en el fichero.

La contestación se realizará por el mismo medio de comunicación utilizado por el afectado para realizar su solicitud.

# 10. PRINCIPIOS RELATIVOS AL TRATAMIENTO

## 10.1. Objetivo

Declarar los principios y los requisitos derivados del RGPD y la LOPD que son declarados principios y requisitos del GRUPO SEPIDES-, y sin los cuales no podrá realizarse ningún tratamiento.

Cuando existan dudas respecto a estos principios y requisitos, deberá consultarse o buscar el asesoramiento del Delegado de Protección de Datos.

## 10.2. Principios Generales de Tratamiento

De conformidad con la normativa de protección de datos, para que desde el GRUPO SEPIDES podamos realizar un tratamiento de datos personales, deberemos cumplir con los siguientes principios.

- Principio de licitud, lealtad y transparencia.
- Principio de limitación de la finalidad.
- Principio de minimización de datos.
- Principio del plazo de conservación.
- Principio de responsabilidad proactiva.
- Principio de integridad y seguridad.

Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

Debemos mantener de manera constante y plena el principio de transparencia, de manera que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Se buscará el medio más adecuado para dar cumplimiento a este principio, pudiendo incluso emplear un modo verbal para dar cumplimiento al mismo.

Daremos cuentas al interesado sobre la identidad del responsable (nuestros datos y en su caso los de los corresponsables) y los fines del mismo. Daremos información sobre el tratamiento leal y transparente y su derecho a obtener confirmación y comunicación de sus datos personales que sean objeto de tratamiento.

Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos ante nosotros.

No aceptaremos fines no específicos en el tratamiento de datos personales. Los fines serán explícitos y legítimos, y se determinarán en el momento de su recogida.

Solo trataremos los datos personales que sean adecuados, pertinentes y limitados a lo necesario para los fines.

El tratamiento de datos, estará limitado a un plazo de conservación. Para garantizar que los datos personales no se conservan más tiempo del necesario, dispondremos de un procedimiento asociado a la política de calificación de la información. Estableceremos un proceso para revisar y procesar un expurgo de información, cuando se hubiera cumplido el plazo determinado. Se eliminarán todos aquellos datos que no se encuentren actualizados, que sean inexactos o que no sean necesarios para el tratamiento.

Los datos personales deben tratarse de un modo que garantice la seguridad y confidencialidad de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos.

## 10.3. Licitud en el Tratamiento

Todo tratamiento de datos que realicemos, necesita apoyarse en una base que lo legitime. Podremos considerar como base, las siguientes:

- Consentimiento.
- Relación contractual.
- Intereses vitales del interesado o de otras personas.
- Obligación legal para el responsable.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

Como responsables analizaremos siempre la licitud, y la declararemos en el registro de tratamiento de actividades. La identificación de la base legal es indispensable para estar en condiciones de demostrar que cumplimos con las previsiones del RGPD. La identificación y documentación debe adaptarse al tipo de tratamiento y a las características de las organizaciones.

Incluiremos la base legal sobre la que se desarrolla el tratamiento al proporcionar la información en el momento de recoger los datos de los interesados.

Se podrá realizar un tratamiento cuando;

a) Se ha prestado consentimiento para uno o varios fines específicos.

b) Si el tratamiento es necesario para la ejecución de un contrato en el que sea parte o para la aplicación a petición del interesado de medidas precontractuales.

c) Si el tratamiento es necesario para satisfacer los intereses legítimos del responsable o por un tercero, siempre que no prevalezcan los intereses o derechos/ libertades del titular de los datos.

d) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable como responsable del tratamiento.

e) El tratamiento es necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

f) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.

**Interés Legítimo**

Especificaremos y documentaremos los intereses legítimos en que se fundamentan las operaciones de tratamiento.

El interés legítimo se puede utilizar como base de licitud de un tratamiento "siempre que no prevalezcan los intereses o los derechos y libertades de la persona interesada" y teniendo en cuenta las expectativas razonables de las personas afectadas por el tratamiento, basadas en la relación que tienen con el Responsable del Tratamiento.

El uso del interés legítimo como base de licitud del tratamiento debe ser evaluado adecuadamente, tomando en consideración que cuando la licitud del tratamiento se basa en el interés legítimo del responsable del tratamiento (o de un tercero), hay que sopesar estos intereses y los de las personas que se verán afectadas.

Para poder considerar que nuestra base de licitud, de interés legítimo puede ser adecuada y conforme, deberemos considerar la realización de un análisis y una ponderación adecuada.

**Consentimiento**

Cuando la base de licitud del tratamiento es el consentimiento del interesado, el responsable del tratamiento debe poder garantizar y demostrar que ha obtenido el consentimiento inequívoco y libre según las directrices del Grupo de trabajo del art. 29 otorgadas en el documento 'WP259 Directrices sobre el consentimiento' en virtud del Reglamento General de Protección de Datos.

El consentimiento debe ser "inequívoco" El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa.

No se admiten formas de consentimiento tácito o por omisión, basadas en la inacción del interesado.

Además, deberá ser "explícito", para tratamientos de datos sensibles, adopción de decisiones automatizadas, y transferencias internacionales.

Cuando requiramos el consentimiento, procuraremos hacerlo por escrito o empleando un medio equivalente, y siempre presentaremos de manera diferenciada los diferentes puntos sobre los que debe procurarse el consentimiento. Se buscará que el consentimiento sea otorgado, de forma inteligible y usando un lenguaje claro y sencillo.

Se podrá revocar el consentimiento en cualquier momento y, además, de forma sencilla.

Como responsable, mantendremos una capacidad de acreditar que los interesados han otorgado su consentimiento para el tratamiento de sus datos personales.

No se recogerá el consentimiento, cuando se disponga de otra base legal que permita el tratamiento de los datos.

**Tratamiento de menores de edad**

Por defecto, el GRUPO SEPIDES no requiere la recogida de datos personales de menores de edad. No obstante, cuando debamos recoger datos personales de menores de edad, se requerirá el consentimiento de los progenitores o tutores.

**Tratamiento de categorías especiales de datos.**

Con carácter general no podremos realizar el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexuales de una persona física salvo:

a) la persona afectada nos haya dado su consentimiento.

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del Derecho laboral y de la seguridad y así lo autorice el Derecho de la Unión o un convenio colectivo.

c) el tratamiento es necesario para proteger intereses vitales de la persona afectada o de otra persona física, en el supuesto de que la persona interesada no esté capacitada, física o jurídicamente, para dar su consentimiento.

d) el tratamiento se refiere a datos personales que la persona interesada ha hecho manifiestamente públicos.

e) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

f) el tratamiento es necesario por razones de un interés público esencial

g) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria.

## 10.4. Deber de Transparencia e Información a los Interesados

La información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Se deberán evitar las fórmulas confusas, excesivamente jurídicas y farragosas y que incorporen remisiones a normas. Las cláusulas informativas deberán explicar el contenido al que se refieren de forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia. Daremos información en modo escrito y cuando fuera posible, mediante medios electrónicos. Nuestro deber de información incluye necesariamente, los siguientes puntos;

- Base jurídica del tratamiento.
- Intención de realizar transferencias internacionales.
- Datos del Delegado de Protección de Datos.
- Elaboración de perfiles y decisiones automatizadas.

Además, incluiremos; la información como responsable, los destinatarios de los datos, plazo de conservación, derechos de las personas afectadas, reclamaciones pertinentes, la obligación de facilitar datos y consecuencias de la negativa.

# 11. PROCEDIMIENTO DE GESTIÓN DEL RIESGO

## 11.1. Objetivo

Definir el procedimiento de gestión de riesgos en la privacidad, enfocándose desde la perspectiva legal y con base en el requerimiento impuesto por la legislación, para el GRUPO SEPIDES.

Este procedimiento determina el modo de realización del análisis de riesgos conforme al artículo 32 del RGPD y la evaluación de impacto conforme al artículo 34 del RGPD.

## 11.2. Alcance

Se considera como alcance el GRUPO SEPIDES y las operaciones de tratamiento del mismo. Se considera que cuando existan corresponsabilidades, cada corresponsal deberá realizar su propio análisis de riesgos.

## 11.3. Gestión de los Riesgos

En base al considerando 76 del RGPD *"La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto".*

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. La gestión del riesgo forma parte de la Responsabilidad Proactiva del Responsable.

Considerando el RGPD,

- En algunos casos, solo realizaremos determinadas medidas cuando el tratamiento suponga un alto riesgo para los derechos y libertados (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
- En otros casos, las medidas las modularemos en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Gestionar los riesgos implica, identificarlos, evaluarlos y tratarlos. Para evaluar el riesgo, hay que llevar a cabo tres tipos de actividades:

1. Las que tienen por objeto identificar el origen de los riesgos, es decir, reflexionar sobre los potenciales escenarios de riesgo a los cuales pueden estar expuestas los datos personales.

2. El análisis de las situaciones que generan riesgo, teniendo en cuenta los diversos factores y características que pueden entrar en juego a la hora de determinar el nivel de riesgo que implican.

3. La valoración de los riesgos, teniendo en cuenta la probabilidad que un acontecimiento no deseado se produzca y la gravedad que puede tener (consecuencias potenciales).

Las operaciones de tratamiento de los datos personales, cuando GRUPO SEPIDES, ocupa la posición jurídica de responsable del tratamiento, se han agrupado en un Registro de Actividades en cumplimiento de las disposiciones del Reglamento General de Protección de Datos y, en concreto, de su artículo 30.

Los distintos registros creados se hacen en función de las diferentes operaciones en las que se tratan datos personales con una finalidad común, además se incluyen aquellas que la Agencia Española de Protección de Datos Personales (en adelante AEPD) señala como necesarias en todas las organizaciones que son las referidas a las notificaciones de brechas de seguridad y el ejercicio de derechos de los interesados.

Considerando estos registros, se ha establecido la gestión de riesgos, que podrá segregarse en diferentes procesos de gestión de riesgos, pudiendo emplearse una metodología común o una metodología diferenciada.

La AEPD, en el ejercicio de sus funciones como autoridad de control, ha puesto a disposición de las empresas una serie de Guías y herramientas (FACILITA) que permite cumplir con el RGPD en tratamientos de bajo riesgo para los derechos y libertades de los afectados. Cuando uno de los tratamientos, se pueda considerar, siguiendo los criterios de la AEPD como un tratamiento de bajo riesgo, se podrá emplear la herramienta FACILITA para gestionar el riesgo.

No obstante, GRUPO SEPIDES considera la gestión del riesgo desde una perspectiva única empleando la metodología descrita.

## 11.4. Metodología de Análisis de Riesgo

Se desarrolla un análisis de riesgos en una plantilla en EXCEL. Se deben identificar las operaciones de tratamiento y se definirán los riesgos por defecto que se declaran presentes en los tratamientos.

Estos riesgos se identificarán desde la dimensión de Protección de Datos Personales y desde la dimensión de Derechos y Libertades de los Interesados.

Se considerarán las medidas de control establecidas previamente como elementos de control de los riesgos y se valora la probabilidad y el impacto en caso de materializarse los riesgos.

La metodología utilizada se basa en los criterios de las autoridades de control y, en concreto, en la "Guía de Gestión del Riesgo y evaluación de impacto en tratamiento de datos personales" de la Agencia Española de Protección de Datos publicada en junio de 2021.

Para la cuantificación del riesgo, se considerarán los valores de la siguiente matriz;

| Impacto | |
|---|---|
| Nivel de impacto | Descripción |
| Muy significativo | Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución y sus consecuencias son irreversibles y/o |

| | |
|---|---|
| | Las consecuencias están relacionadas con las categorías especiales de datos o relativos a infracciones penales, y es irreversible, y/o<br>Causa un daño social significativo, como la discriminación, y es irreversible u/o<br>Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible y/o<br>Causa pérdidas morales o materiales significativas e irreversibles |
| Significativo | Los casos anteriores cuando los efectos son reversibles y/o<br>Pérdida del control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos y/o<br>Se produce o puede producirse usurpación de la identificar de los interesados y/o<br>Pueden producirse pérdidas significativas a los interesados y/o<br>Pérdida de la confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad y/o<br>Existe un perjuicio social para los interesados o determinados colectivos de interesados |
| Limitado | Pérdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter reversible y/o<br>Perdidas financieras insignificantes o irreversibles y/o<br>Pérdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penal |
| Muy limitado | En el caso anterior, cuando todos los efectos son reversibles |

| PROBABILIDAD | |
|---|---|
| PROBABILIDAD | DESCRIPCIÓN |
| Improbable | Si no hay constancia de materialización de dicho riesgo en ningún caso. |
| Baja | Si hay constancia de una materialización de dicho riesgo en los últimos 10 años. |
| Alta | Si hay constancia de una materialización de dicho riesgo en el último año<br>y/o<br>Existen estudios que determinan que la probabilidad podría ser alta.<br>y/o<br>Existen auditorías/estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.<br>y/o<br>Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes |
| Muy alta | Si el factor de riesgo está materializado y no depende de la probabilidad, p.ej. porque la Directrices wp248 identifican el uso de una tecnología como un riesgo y está presente en el tratamiento yo,<br>Si hay constancia de diversas materializaciones de dicho riesgo en el último año en distintas y/o<br>Si hay constancia de una materialización de dicho riesgo en el último año en la misma entidad. y/o<br>Existen auditorías/estudios que identifican importantes vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. |

Una vez calculado el riesgo, se deberá proceder a una gestión del mismo, con un plan de acción, donde se detallarán las medidas concretas para controlar los riesgos y el área responsable. Deberá realizarse un seguimiento de las medidas y de su eficacia. Analizar al menos una vez al año, los resultados obtenidos mediante las medidas o controles.

Se deberán considerar sobre los riesgos, medidas de tratamiento, que permitan su gestión y reducir su presencia. Debe gestionarse el riesgo, mediante las medidas implantadas. Pueden emplearse medidas del Anexo A de la ISO 27001 o Anexo II Real Decreto 311/2022, o cualquier otro estándar aceptado.

## 11.5. Evaluación de Impacto

Cuando sea probable que un tratamiento o un nuevo producto o un servicio, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, GRUPO SEPIDES, como responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento.

Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

Se ha incluido en nuestra plantilla de análisis de riesgos un punto para evaluar la necesidad de la realización de evaluación de impacto.

Si de la sección de evaluación de requisitos de evaluación de impacto se deduce la necesidad de realizarse, deberá ejecutarse el análisis de impacto. Para ello, deberemos emplear la sección específica de nuestra plantilla.

El artículo 35.3 del RGPD describe los siguientes casos en los cuales se ha considerado que un tratamiento puede derivar en riesgos elevados:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado como la elaboración de perfiles y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos personales, o datos sobre condenas e infracciones penales o medidas de seguridad conexas.
- Observación sistemática a gran escala de una zona de acceso público.

Adicionalmente, con el objetivo de poder determinar qué tipo de tratamientos pueden considerarse de alto riesgo, el grupo de trabajo del artículo 29(GT29) en el documento WP248 Directrices sobre las Evaluaciones de Impacto en la Protección de Datos introduce criterios que pueden evidenciar un elevado riesgo inherente a las actividades de tratamiento y que, se deben evaluar y pueden determinar la necesidad de realizar una evaluación de impacto (PIA):

| TIPO DE TRATAMIENTO | DESCRIPCIÓN |
|---|---|
| Evaluación o scoring | Valoraciones y análisis, incluidos la elaboración de perfiles y predicciones, especialmente de "aspectos relacionados con el desempeño del interesado en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos". |
| Toma de decisiones automatizada con efecto legal o similar | Procesamiento que tiene como objetivo la toma de decisiones sobre sujetos que producen "efectos legales sobre la persona física" o que "de manera similar afecta significativamente a la persona física". Por ejemplo, si el procesamiento puede conducir a la exclusión o discriminación de las personas. |
| Monitorización sistemática | Procesamiento utilizado para observar o controlar a los interesados, incluidos los datos recopilados a través de redes o un sistema de control de un área de acceso público. |
| Datos confidenciales o de naturaleza altamente personal | Actividades de tratamiento con categorías especiales de datos personales, por ejemplo, información sobre las opiniones políticas de los individuos o registros médicos, así como datos personales relacionados con condenas penales o delitos. |
| Coincidencia o combinación de conjuntos de datos | Actividades de tratamiento que implican la combinación de conjuntos de datos. Por ejemplo, procedentes de dos o más actividades de tratamiento de datos realizadas para diferentes propósitos y/o por diferentes responsables del tratamiento de una manera que exceda las expectativas razonables del sujeto de datos. |
| Datos relativos a las personas vulnerables | Los sujetos de datos vulnerables pueden incluir menores, segmentos más vulnerables de la población que requieren protección especial (personas con enfermedades mentales, solicitantes de asilo o ancianos, pacientes, etc.). |
| Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas | Actividades de tratamiento realizadas mediante el uso de tecnología innovadora que pueda implicar nuevas formas de recopilación y uso de datos, posiblemente con un alto riesgo para los derechos y las libertades de las personas. Por ejemplo, la combinación del uso de la huella dactilar y el reconocimiento facial para mejorar el control del acceso físico, etc. |
| Cuando el procesamiento en sí mismo "impide que los interesados ejerzan un derecho o utilicen un servicio o un contrato" | Operaciones de procesamiento que tienen como objetivo permitir, modificar o rechazar el acceso de los interesados a un servicio o la entrada en un contrato. |

| TIPO DE TRATAMIENTO | DESCRIPCIÓN |
|---|---|
| Tratamientos sujetos a un código de conducta que lo requiere | Si a los tratamientos evaluados se les aplica un código de conducta que exige su cumplimiento también debe ser objeto de la evaluación. |

Asimismo, la autoridad de control podrá establecer listas relacionadas con los tipos de tratamiento que necesariamente impliquen una evaluación de impacto, o en su caso, que por defecto no lo requieran:

**Supuestos de la autoridad de control que no requieren una evaluación.**

**1.** Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.

**2.** Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.

**3.** Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

**4.** Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos, o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.

**5.** Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.

**6.** Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.

**7.** Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

Si de los resultados de la evaluación de impacto se extrae un riesgo elevado, deberá considerarse lo descrito en el artículo 36 del RGPD. Como responsable, consultaremos a la autoridad de control antes de proceder al tratamiento cuando de la evaluación de impacto, se deriva que un tratamiento entrañaría un alto riesgo si no se adoptan medidas para para mitigarlo.

## 11.6. Roles y Responsabilidades

La definición de roles y responsabilidades de quienes deben realizar y valorar los resultados en relación con la gestión de riesgos, se realizará de acuerdo a la siguiente distribución:

- (R) RESPONSABLE DE LA TAREA: Persona a la que se le asigna la función o acción específica.
- (A) QUIEN DEBE CONTROLADOR SU EJECUCIÓN: Propietario que debe asumir las responsabilidades.
- (C) A QUIEN SE PUEDE CONSULTAR: Delegado de Protección de Datos.
- (I) A QUIEN SE DEBE INFORMAR: Área impactada por una responsabilidad o acción.

| FASE | RESPONSABLE DEL TRATAMIENTO | DPD | ENCARGADO DEL TRATAMIENTO | OTRAS ÁREAS RELEVANTES) |
|---|---|---|---|---|
| a) Describir el ciclo de vida de los datos | R/A | C/I | C | C |
| b) Analizar la necesidad y proporcionalidad del tratamiento | R/A | C/I | C | C |
| c) Identificar amenazas y riesgos | R/A | C/I | C | |
| d) Análisis de los riesgos | R/A | C/I | C | |
| e) Plan de Tratamiento de Riesgos | R/A | C/I | C | C |

## 12. POLÍTICA Y PROCEDIMIENTOS SEGURIDAD DE LA INFORMACIÓN

La Dirección de SEPIDES, en el marco de cumplimiento y certificación del Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad, ha establecido una Política de Seguridad de la Información y unas normas y procedimientos de seguridad con el objetivo de mantener, administrar, recolectar, recuperar, procesar, almacenar y distribuir la información que precisamos en nuestros servicios. Además, consideramos a todos los usuarios, datos personales e información no personal, recursos y activos tangibles e intangibles y todas las instalaciones de tratamiento. Se presta especial atención a todos los activos de carácter tecnológico, incluyendo los suministros, sin los cuales no podemos garantizar la continuidad y resiliencia de los sistemas.

En la documentación elaborada en el ámbito de la Seguridad de la Información, se ha establecido, entre otros, los siguientes aspectos:

- Principios y Objetivos de la Seguridad de la Información.
- Organización de la Seguridad de la Información (comités y responsables).
- Manual del Sistema de Gestión de Seguridad de la Información (SGSI).
- Manual de Políticas y Normas, en la que se desarrolla:
  - Gestión de personal.
  - Equipamiento informático.
  - Correo electrónico e Internet.
  - Protección de la información.
  - Acceso a edificios e instalaciones.
- Manual de Procedimientos e Instrucciones Técnicas de Tecnologías de la Información, en la que destacamos:
  - Gestión de accesos a sistemas de información.
  - Gestión de peticiones e incidencias de sistemas de información.
  - Gestión de autorizaciones y cambios.
  - Gestión de activos.
  - Gestión de logs (actividad de los usuarios).
  - Gestión de la configuración y capacidad.
  - Gestión de desarrollos y mantenimientos.
  - Gestión de copias de seguridad.
  - Gestión de soportes de información.
  - Gestión de antivirus.
  - Gestión de servicios externos.

Esta documentación estará disponible para el personal de la organización para su conocimiento y correcta aplicación.

# 13. POLÍTICA DE GESTIÓN DOCUMENTAL

## 13.1. Objetivo

Establecer unas pautas comunes para mantener la seguridad de los datos personales que se encuentren en soporte documental. Para garantizar el nivel de protección exigido en el RGPD, son de aplicación una serie de normas, procedimientos y estándares relacionados con la seguridad en los locales y fuera de las instalaciones del GRUPO SEPIDES. Así mismo, y complementariamente a las pautas aquí desarrolladas, la Dirección ha establecido una norma de carácter general a toda la organización sobre la Gestión de la Documentación de la compañía y la cual igualmente estará accesible al personal para su correcta aplicación (Procedimiento de Gestión de la Documentación del Sistema de **Gestión de Seguridad de la Información**)

## 13.2. Desarrollo

### 13.2.1. Control de acceso

Se mantendrá el principio de segregación y solo los usuarios con acceso previo podrán acceder a los datos en soporte en papel. Solo tendrán acceso a aquellos datos que precisen para el desarrollo de sus funciones.

Se establecerán mecanismos de archivo temporal controlados por personal con autorización expresa mientras se encuentren en uso y se mantendrá un archivo permanente cuando la información deje de ser necesaria. Los accesos a este archivo estarán controlados.

El acceso por parte de otras personas estará estrictamente prohibido, y únicamente podrá producirse mediante petición firmada del interesado y autorización por escrito del Delegado de Protección de Datos.

El personal ajeno al GRUPO SEPIDES con acceso a los locales y recursos ámbito de la presente Política está sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

### 13.2.2. 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, supresión y limitación. Esta información se alineará con la política de calificación de la información de la compañía.

Los criterios de archivo de la documentación, garantizarán la conservación, la localización, la consulta y el ejercicio de los derechos legalmente reconocidos.

Los plazos de conservación de la información personal, quedara descrita en el Registro de Actividades de Tratamiento y será informada a los usuarios, cuando se realicen las acciones de información y transparencia o cuando se ejerzan los correspondientes derechos.

Cuando no exista norma aplicable, GRUPO SEPIDES establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo. Corresponde la definición de dichos criterios a la dirección de GRUPO SEPIDES o al responsable del área o departamento en cuestión, con el apoyo de los responsables competentes. Se contará con el asesoramiento del Delegado de Protección de Datos y del Responsable de Seguridad.

Con carácter general la entidad aprobará a nivel de grupo o a nivel individual de las sociedades, una política de calificación de la información, considerando lo dispuesto en la normativa aplicable a la naturaleza de la información.

Se establecerán medidas de seguridad tras calificar la información.

### 13.2.3. Criterios para la delimitación de plazos

La limitación del plazo de conservación de los datos de carácter personal, constituye uno de los principios básicos establecidos en el Reglamento General de Protección de Datos, en concreto, su artículo 5.1 (e) establece, que los datos personales serán 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.

Podrán, sin embargo, mantenerse por plazos más largos, siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone Reglamento, a fin de proteger los derechos y libertades del interesado.

Se debe de tener en cuenta, además, el principio de información, que exige al Responsable de Tratamiento informar a los afectados, del plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

**Criterios de para establecer plazos**

Lo plazos de conservación de los datos de carácter personal tratados por la organización, están ligados a la tipología de datos tratados, así como a la finalidad para la cual se han recabado.

El establecimiento de los plazos de conservación, está vinculado a distintos factores, entre los que se encuentran los siguientes:

- **Finalidad para la cual se han recabado los datos**: Los datos de carácter personal tratados por la entidad, se recaban con unos fines concretos (establecimiento de una relación, inicio de una relación laboral, realización de acciones de marketing etc.), y se deberán mantener durante no más tiempo del necesario para los fines del tratamiento.
- **Existencia de una ley**: En ocasiones, los plazos de conservación vienen establecidos en una ley, debiendo la entidad conservar los datos de carácter personal, durante los plazos que exige la normativa aplicable en cada caso. Por ejemplo, los datos relativos a los trabajadores están sujetos a una relación contractual o funcionarial. Una vez finalizada la relación laboral, se extinguirá la finalidad para la cual se han recabado los datos tratados, pero, sin embargo, deberán mantenerse más allá de dicha relación, con el objeto de depurar responsabilidades.

- **Principios establecidos en el Reglamento General de Protección de Datos (RGPD)**: En otras ocasiones, si bien el plazo no está establecido en una ley, viene derivado de la existencia de otros principios básicos establecidos en el Reglamento General de Protección de Datos, tales como el principio de exactitud, que exige el mantenimiento de los datos de manera exacta y actualizada.
- **Interés legítimo**: Si se desea mantener los datos de carácter personal una vez finalizados los fines para los que se recabaron y más allá de los plazos legales establecidos, deberá valorarse si existe un interés legítimo en su mantenimiento. Sin perjuicio de que previamente se deba realizar un examen del interés legítimo con el objeto de conocer, si es posible o no el mantenimiento de los mismos. Un ejemplo de este supuesto, sería el mantenimiento de un registro histórico del personal de una organización.

Los plazos de conservación que afectan a las distintas tipologías de datos de carácter personal, no dependen de un único factor y se deberá tener en cuenta, no sólo los fines para los cuales han sido recabados sino también, los plazos legales que pueden afectar a las distintas tipologías de datos, así como otras circunstancias que sean susceptibles de afectar a la organización (Tales como el interés legítimo, el ejercicio del derecho de oposición al tratamiento etc.).

**Bloqueo de datos**

El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

GRUPO SEPIDES, solamente podrá proceder al bloqueo de datos de carácter personal, cuando se prevea en una norma con rango de ley. El bloqueo podrá efectuarse durante los plazos de prescripción establecidos en la normativa que resulte de aplicación y con la finalidad de exigencia de posibles responsabilidades derivadas del tratamiento.

### 13.2.4. Periodos de almacenamiento.

El calendario de plazos de conservación y bloqueo, ha sido trazado sobre los Registros de Actividades. El calendario de plazos de conservación se encuentra definido en **SGAJ.PRO.19.001-1.2 Gestión de la Documentación.**

En cuanto a la destrucción de la documentación, la misma se llevará a cabo previa autorización de la Administración competente conforme a lo contemplado en el art. 55 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español

### 13.2.5. Eliminación y destrucción de la información

Los empleados de la organización que manejan documentos individuales son responsables de destruir los soportes en papel, salvo que la Política de clasificación de la información clasificada establezca otra cosa. Los soportes en papel se destruyen manualmente.

## 13.2.6. Dispositivos de almacenamiento y archivos

**a) Mecanismos de protección**

Los dispositivos de almacenamiento 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, se adoptarán medidas que impidan el acceso de personas no autorizadas.

**b) Ubicación de los dispositivos de almacenamiento.**

Los armarios, archivadores u otros elementos en los que se almacene información 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. Si, atendidas las características de los locales, no fuera posible cumplir con esto se adoptarán medidas alternativas. Estas circunstancias, constaran en el Análisis de Riesgos.

**c) Copia o reproducción y desecho de documentos**

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.

**d) Custodia de documentos**

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos 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.

## 14. ACTUALIZACIÓN Y REVISIÓN DEL PROTOCOLO DE SEGURIDAD

El presente Protocolo será actualizado y revisado en el caso de que se produzcan cambios en el sistema de información o en la empresa, y, en cualquier caso, se adecuan a las disposiciones legales vigentes en materia de protección de datos de carácter personal.

Mantendremos una seguridad proactiva y gestionaremos la seguridad de los datos de manera permanente. Para ello, se revisará el cumplimiento de las obligaciones derivadas de la normativa y del grado de efectividad y eficacia de las medidas de seguridad técnica y organizativa, a intervalos planificación y con la mayor objetividad posible.

El equipo que participa en el diseño e implantación de las medidas de seguridad no podrá comprobar el grado de eficiencia y eficacia de las mismas, en base al principio de segregación de funciones y separación de tareas.

Todo el personal permitirá y contribuirá a las revisiones desarrolladas para comprobar el grado de cumplimiento de las revisiones del sistema, inspecciones y auditorias.

Todo proveedor pondrá a disposición del personal propio o de terceros encargado de realizar nuestras revisiones, toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, permitiendo y contribuyendo a la realización de auditorías, inspecciones y revisiones in situ o en remoto.

El DPD supervisará las operaciones de tratamiento afectadas y en concreto las auditorias o revisiones correspondientes. El DPD, debe mantener una vigilancia exhaustiva respecto al cumplimiento de la normativa implicada, y especialmente de la responsabilidad proactiva del responsable, incluyendo la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes para evidenciar la diligencia de la organización. Podrá realizar diferentes acciones de verificación, incluyendo inspecciones, cuestionarios de diligencia, entrevistas y procesos de auditoría.

El DPD se encargará de preparar un plan de auditoría a nivel de grupo, de manera que anualmente y siempre por muestro, las entidades del grupo sean revisadas y puedan acreditar el nivel de adecuación de sus medidas a la exigidas. En un ciclo de tres años, deberán ser revisadas las entidades del grupo. Las auditorias podrán ser realizadas por terceros de manera que se garantice la objetividad e imparcialidad de los resultados.

A nivel de grupo, las presentes medidas y cuantas otras sean desarrolladas para dar cumplimiento a este documento, serán consideradas obligatorias a nivel de grupo, y entre ellas las de someterse a medidas de verificación del cumplimiento de las mismas. Se incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberán comunicarse al consejo de administración de la empresa matriz / que controla un grupo empresarial, y en su caso ponerse a disposición de la autoridad de control competente que lo solicite.

Todos los resultados de estos procesos de revisión, incluidas las auditorias relacionadas con protección de datos y acciones correctivas desarrolladas para proteger los datos personales, serán comunicadas a la Alta Dirección – Consejo de Administración y en su caso, estarán a disposición de la autoridad de control competente.

# 15. PROCEDIMIENTO DE GESTIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS

El objetivo de este procedimiento es definir y normalizar un procedimiento que permita la gestión de violaciones de seguridad que afecten a datos personales y en su caso, su notificación según corresponda (a la Agencia Española de Protección de Datos y/o a los interesados), y su comunicación ( a los interesados) de acuerdo con la normativa de protección datos personales, de modo que se asegure su documentación, priorización, gestión reactiva / preventiva optimizando su gestión y promoviendo el aprendizaje. El procedimiento de violaciones de seguridad de datos está definido en el Procedimiento de Gestión de Incidentes de Seguridad del Sistema de Gestión de Seguridad de la Información.

# 16. ROLES Y RESPONSABILIDADES EN PROTECCIÓN DE DATOS

## 16.1. Objeto

La seguridad deberá comprometer a todos los miembros de la organización, en base a sus diferentes roles, considerando diferentes responsabilidades.

La Dirección será quien lidere la organización y promueva la cultura de seguridad y legalidad, asignando los roles requeridos y potenciando la transversalidad de la seguridad en cada proceso o servicio desarrollados.

Con carácter general se deriva la seguridad al Comité de Seguridad con inclusión de los responsables de privacidad que se describen en este documento.

La seguridad del sistema será revisada de conformidad a los requisitos, la política y los procedimientos aprobados.

## 16.2. Delegado de Protección de Datos

En el marco del sistema desarrollado en el GRUPO SEPIDES, en materia de protección de datos, establece una estructura organizativa con responsabilidades diferenciadas y específicamente, se crea la figura del Delegado de Protección de Datos, en adelante DPD. El Delegado de protección de datos podrá estar integrado en órganos de seguridad con funciones propias.

El objeto de la misma es dar cumplimiento a la normativa de protección de datos personales.

A pesar de que GRUPO SEPIDES no está obligado a designar un DPD de acuerdo con lo establecido en el Art. 37 del RGPD y Art. 34 de la LOPD, es recomendable su designación. La organización asume la posibilidad de realizar acciones con carácter previo a las actuaciones de la Autoridad de Control, cuando un tercero realice acciones de reclamación ante la misma. Cuando el afectado presente una reclamación ante la Autoridad de Control de protección de datos, ésta podrá remitir la reclamación a nuestro delegado de protección de datos a fin de que este responda en el plazo de un mes.

El objetivo de la creación de la figura es facilitar el cumplimiento de la normativa mediante la implementación de herramientas de rendición de cuentas (evaluaciones de impacto y auditorías), así como actuar de intermediario entre las partes interesadas

correspondientes (autoridades supervisoras, interesados y Departamentos de empresas del GRUPO SEPIDES).

GRUPO SEPIDES pondrá a disposición del DPD los medios adecuados (línea directa, línea directa específica o formulario de contacto específico dirigido al DPD en el sitio web de GRUPO SEPIDES u otros medios de comunicación seguros), para garantizar que los interesados puedan ponerse en contacto con él. El DPD está obligado a mantener secreto documental y confidencialidad en relación con el desempeño de sus tareas. No obstante, dicha obligación no prohíbe al DPD entrar en contacto con la autoridad supervisora o pedirle asesoramiento.

El rol de Delegado de Protección de Datos, tendrá una designación formal. Su finalidad será mantener el cumplimiento y garantizar que la organización desarrolle sus actividades principales conforme a los principios legales y la presente política.

El Delegado ejercerá sus funciones en paralelo con la seguridad de la información, debiendo informar al Responsable de Seguridad, de brechas relacionadas con la privacidad o elementos de incumplimiento que estén afectando al entorno legal.

## 16.3. Perfil del DPD

El perfil de la persona designada dentro de GRUPO SEPIDES como DPD deberá cumplir los siguientes requisitos:

- Conocimiento acorde a GRUPO SEPIDES de las leyes y prácticas de protección de datos tanto nacionales como europeas y una comprensión profunda del RGPD.
- Conocimiento acorde a GRUPO SEPIDES del sector empresarial y la organización.
- Comprensión acorde a GRUPO SEPIDES de las operaciones de tratamiento llevadas a cabo y los sistemas de información, así como las necesidades de seguridad y protección de los datos.
- Elevada capacidad de desempeño basada en la integridad y la ética profesional.

El Delegado, "se designará sobre la base de cualidades profesionales y, en particular, el conocimiento experto de la legislación y prácticas de protección de datos y la capacidad para cumplir las tareas encomendadas". Se considerará en todo caso, las incompatibilidades potenciales y se asignará siempre a una persona que no pueda incurrir en un conflicto de intereses.

Con el objetivo de garantizar que los interesados (tanto dentro como fuera de la organización) y las autoridades supervisoras puedan ponerse en contacto con el DPD de forma fácil, directa y confidencial, cumpliendo así con el Art. 37 del RGPD, GRUPO SEPIDES:

- Publicará los datos de contacto genéricos del DPD y
- Comunicará los datos de contacto del DPD a las autoridades supervisoras correspondientes.

## 16.4. Puesto del DPD

El DPD será nombrado por el Consejo de Administración de SEPIDES, recogiéndose su nombramiento y confiriéndole suficiente autonomía en un acta.

Desarrollará sus funciones por un periodo de 3 años y una vez transcurridos, el Consejo de Administración de SEPIDES podrá optar por proponer su continuidad o presentar a un nuevo candidato.

Con el fin de garantizar que el DPD se involucre, de manera adecuada y oportuna, en todas las cuestiones que guarden relación con la protección de los datos personales de GRUPO SEPIDES, la organización garantizará que:

- Se invita al DPD a participar en reuniones con los directivos altos y medios.
- Está presente cuando se tomen decisiones con implicaciones para la protección de datos. Toda la información relevante debe transmitirse al DPD de manera oportuna para que pueda prestar un asesoramiento adecuado.
- Goza de la consideración debida. En caso de desacuerdo, se documentarán las razones de no seguir su consejo.
- Se consulta al DPD en caso de violación de datos u otro incidente.

En su caso, GRUPO SEPIDES elaborará directrices o programas de protección de datos que determinen cuándo debe consultarse al DPD.

Por otro lado, la organización respaldará al DPD, en base al Art. 38 del RGPD, proporcionando los recursos necesarios para que lleve a cabo sus tareas y acceda a los datos personales y las operaciones de tratamiento.

En especial, GRUPO SEPIDES respaldará en los siguientes aspectos:

- Apoyo activo a la función del DPD por parte de la alta dirección.
- Asegurar tiempo suficiente para que el DPD cumpla con sus funciones.
- Comunicación oficial de la designación del DPD a todo el personal de GRUPO SEPIDES para asegurar que su existencia y su función se conozcan dentro de la organización.
- Acceso necesario a otros servicios, tales como recursos humanos, TI, seguridad, etc., de modo que el DPD pueda recibir apoyo esencial, datos e información de esos otros servicios.
- Formación continua.

Asimismo, GRUPO SEPIDES establece unas garantías suficientes para ayudar a asegurar que el DPD lleva a cabo sus tareas con el suficiente grado de autonomía dentro de su organización. En este sentido, el DPD no recibirá instrucciones sobre cómo actuar o sobre una cuestión relacionada con la legislación de protección de datos.

El DPD podrá desistir en su cargo, previa comunicación al Secretario del Consejo de Administración de SEPIDES con una antelación de un mes, alegando los motivos por los que haya decidido no continuar. Asimismo, el Consejo de Administración de SEPIDES, podrá acordar el cambio de DPD, si se detecta que no realiza las labores encomendadas en el presente Reglamento. Este cambio será comunicado por la Dirección al DPD explicando las causas que han llevado a tomar dicha decisión.

El DPD no puede ser destituido ni penalizado por GRUPO SEPIDES por llevar a cabo sus funciones. En caso de sanciones, se aplicarán las contempladas en el sistema disciplinario establecido en la organización para sus diferentes actividades, así como, en el caso de destitución, se atenderá a la misma casuística contemplada para cualquier otro empleado o contratista sujeto a la legislación contractual, laboral o penal aplicable.

Por último, destacar que el DPD desempeñará otras tareas y funciones que no deriven en un conflicto de interés. Así el DPD no podrá detentar un cargo dentro de la organización que le lleve a determinar los fines y medios del tratamiento de datos personales.

## 16.5. Funciones del DPD

Las funciones del DPD de GRUPO SEPIDES son las siguientes:

- Controlar el cumplimiento del RGPD por GRUPO SEPIDES. En este sentido podrá:
  - recabar información para determinar las actividades de tratamiento y configurar el Registro,
  - analizar y comprobar la conformidad de las actividades de tratamiento, e
  - informar, asesorar y emitir recomendaciones a GRUPO SEPIDES.
- Asesorar a GRUPO SEPIDES para llevar a cabo las evaluaciones de impacto de la protección de datos. En este sentido decidirá sobre:
  - si se debe llevar a cabo o no una evaluación de impacto de la protección de datos,
  - qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos,
  - si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa,
  - qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados y
  - si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD.
- Considerar debidamente el riesgo asociado a las actividades de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento:
  - priorizando sus actividades y centrando sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.
  - asesorando sobre cuales áreas deben someterse a auditoría de protección de datos interna o externa,

- recomendando formación interna al personal y directores responsables de las actividades de tratamiento de datos y
- definiendo a qué operaciones de tratamiento dedicar más tiempo y recursos.

- Mantener el registro de las operaciones de tratamiento, responsabilidad de GRUPO SEPIDES con el fin de llevar a cabo las funciones de control del cumplimiento, información y asesoramiento.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

El DPD informará anualmente a la Alta dirección del GRUPO SEPIDES sobre del sistema de protección de datos en relación con:

- Aplicación de medidas desde el diseño y por defecto.
- Revisión del Registro de Actividades de Tratamiento.
- Resultado del análisis de riesgos y de la evaluación del impacto de la protección de datos.
- Plan de Tratamiento de Riesgos.
- Violaciones de seguridad de los datos.
- Plan de formación.
- Procedimientos, normas, cláusulas, contratos.
- Asignación presupuestaria de ejercicio destinada a estos fines.
- Cualquier otra cuestión que el DPD considere oportuna.

Para ello el DPD realizará un informe de revisión del estado de sistema donde se contemplarán los puntos indicados.

## 16.6. Comité de Seguridad

La organización podrá constituir un comité de seguridad, que será el órgano encargado de desarrollar las directrices y estrategia de seguridad. Estará formado por representantes de la Alta Dirección, el Responsable de Seguridad, el Responsable del Sistema y cuando hubiera sido designado, el Delegado de Protección de Datos y el responsable de Seguridad.

La designación de roles se ha establecido a la luz del principio de separación de funciones.

En dicho comité, se presentarán informes detallados relacionados con el nivel de cumplimiento de la normativa y específicamente, de la normativa de protección de datos y del Esquema Nacional de Seguridad.

SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E.

# ANEXOS

Sistema de Protección de Datos

## ANEXO 1: MODELO DE SOLICITUD DE EJERCICIO DE DERECHOS

# MODELO: FORMULARIO DE SOLICITUD DE DERECHOS

1. Datos del responsable del tratamiento para la atención del ejercicio de derecho

| Nombre | NIF | Dirección |
|---|---|---|
| | | |

2. Datos de la persona solicitante

| Nombre y apellidos | | NIF | | |
|---|---|---|---|---|
| | | | | |
| **Dirección (1)** | **Código Postal (1)** | **Población (1)** | **Provincia (1)** | **País (1)** |
| | | | | |
| **Correo electrónico (3)** | | **Teléfono (2)** | **Móvil (3)** | |
| | | | | |

(1) Se deberá señalar la dirección o el domicilio donde se deseen recibir las notificaciones derivadas del ejercicio del presente derecho. (2) Dato optativo. (3) Medio por el cual desea recibir los avisos del envío o puesta a disposición de la notificación (correo electrónico y/o número de dispositivo móvil).

3. Datos del representante

| Nombre y apellidos | | NIF | | |
|---|---|---|---|---|
| | | | | |
| **Dirección (1)** | **Código Postal (1)** | **Población (1)** | **Provincia (1)** | **País (1)** |
| | | | | |
| **Correo electrónico (3)** | | **Teléfono (2)** | **Móvil (3)** | |
| | | | | |

(1) Se deberá señalar la dirección o el domicilio donde se deseen recibir las notificaciones derivadas del ejercicio del presente derecho. (2) Dato optativo. (3) Medio por el cual desea recibir los avisos del envío o puesta a disposición de la notificación (correo electrónico y/o número de dispositivo móvil).

4. Medio de respuesta

Indique el medio por el cual desea que se le comunique la estimación o desestimación de su solicitud de ejercicio de derechos (marque una opción):

☐ Medios electrónicos ☐ Papel

5. Ejercicio del derecho

Seleccione el derecho a ejercer:

| | |
|---|---|
| ACCESO | La persona interesada tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información establecida en el artículo 15 del RGPD. |
| RECTIFICACIÓN | La persona interesada 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, inclusive mediante una declaración adicional, de acuerdo con lo establecido en artículo 16 del RGPD. |
| SUPRESIÓN | La persona interesada tendrá derecho a obtener sin dilación indebida del responsable del Tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir los datos personales cuando concurra alguna de las circunstancias previstas en el artículo 17 del RGPD. |
| OPOSICIÓN | La persona interesada 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 en base a lo establecido en el artículo 21 del RGPD. |
| LIMITACIÓN DEL TRATAMIENTO | La persona interesada tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones establecidas en el artículo 18 del RGPD. |
| PORTABILIDAD DE LOS DATOS | La persona interesada tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin |

| | |
|---|---|
| | que lo impida el responsable al que se los hubiera facilitado, cuando se cumplan algunos de los requisitos establecidos en el artículo 20 del RGPD. |
| TRATAMIENTOS AUTOMATIZADOS | La persona interesada tendrá derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, de acuerdo con lo previsto en el artículo 22 del RGPD. |

Puedes obtener más información en el apartado denominado "Información sobre los derechos".

6. Detalles de la solicitud

Describa para cada una de los derechos seleccionados el detalle sobre los tratamientos y/o información sobre los que desea ejercitarlos en cada caso.

7. Documentación aportada

Descripción de la documentación aportada (nombre documento y breve descripción):

8. Observaciones

En _____ a _____ de _____

Firma,

PROTECCIÓN DE DATOS

| Responsable del tratamiento: SEPI Desarrollo Empresarial S.A.S.M.E (SEPIDES) | Finalidad: Tramitar y gestionar su solicitud del derecho en materia de protección de datos. | Legitimación: El tratamiento se basa en el artículo 6.1 c) del RGPD, tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. | Destinatarios: Están previstas comunicaciones de datos a la Agencia Española de Protección de Datos. | Derechos: Puede acceder, rectificar y suprimir los datos, así como ejercitar otros derechos, cuando procedan, ante SEPIDES, C/Velázquez, 134 28006 Madrid (España), indicando en el asunto: Ref. Protección de Datos | Información adicional: sobre protección de datos en el apartado: **información protección de datos**

# INFORMACIÓN PROTECCIÓN DE DATOS

## Responsable del tratamiento

**Identidad:** SEPI Desarrollo Empresarial S.A.S.M.E. (SEPIDES) con CIF: A-48001382
**Dirección postal:** dirección C / Velázquez 134 Bis – 28006 – Madrid (España)
**Teléfono:** 913 961 461
**DPD:** protecciondedatossepides@sepides.es

## Finalidad del tratamiento:

Finalidad: Los datos recabados a través del formulario, así como otra documentación que pueda ser adjuntada, será tratada con la finalidad de tramitar y gestionar su solicitud del derecho en materia de protección de datos.

Plazos de conservación: Los datos personales se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.

## Legitimación

La base legal para el tratamiento de los datos facilitados, tanto en el formulario como en la documentación que pueda ser adjuntada, se basa en el artículo 6.1 c) del RGPD: tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

## Destinatarios

Están previstas comunicaciones de datos a la Agencia Española de Protección de Datos pudiendo así mismo realizarse otras siempre que se cumplan algunos de los supuestos legalmente previstos en la vigente normativa de protección de datos. No están previstas transferencias internacionales de datos.

## Derechos

Las personas afectadas tienen derecho a:

- Obtener confirmación sobre si SEPIDES está tratando sus datos personales.
- Acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso solicitar la supresión cuando, entre otros motivos, los datos ya no sean necesarios para la finalidad para la que fueron recabados.
- Solicitar en determinadas circunstancias:
  - La limitación del tratamiento de sus datos, en cuyo caso sólo serán conservados por SEPIDES para el ejercicio o la defensa de reclamaciones.
  - La oposición al tratamiento de sus datos, en cuyo caso, SEPIDES dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. Incluyéndose, también, el tratamiento de sus decisiones individuales automatizadas.
  - La portabilidad de los datos para que sean facilitados a la persona afectada o transmitidos a otro responsable, en un formato estructurado, de uso común y lectura mecánica.

Los derechos podrán ejercitarse, cuando proceda, ante SEPIDES, Calle Velázquez 134 Bis-28006 (Madrid) indicando en el asunto: Ref. Protección de Datos.

Si en el ejercicio de sus derechos no ha sido debidamente atendido, podrá presentar una reclamación ante la Agencia Española de Protección de Datos – Dirección: C/Jorge Juan, 6 - 28001 MADRID (Madrid) – Sede electrónica: sedeagpd.gob.es. No obstante, en primera instancia y con carácter potestativo, podrá ponerse en contacto con el Delegado de Protección de Datos en la dirección de correo electrónico: protecciondedatossepides@sepides.es

# INFORMACIÓN SOBRE LOS DERECHOS

## I. Información general

1. El titular de los datos personales objeto de tratamiento debe dirigirse directamente ante SEPI DESARROLLO EMPRESARIAL, S.A., S.M.E (SEPIDES).
2. Se debe identificar de forma inequívoca. Para ello, a la solicitud habrá que adjuntar copia del NIF, NIE, pasaporte o permiso de conducir (en que aparezca la fotografía del titular o) o documento equivalente que acredite la identidad y sea considerado válido en derecho. En caso de que se actúe a través de representación legal deberá aportarse, además, NIF y documento acreditativo de la representación del representante.
3. El ejercicio de derechos será gratuito. No obstante, ante solicitudes infundadas, excesivas o repetitivas por una misma persona afectada en cortos periodos de tiempo, el responsable del tratamiento se podría negar a actuar respecto a dicha solicitud o solicitar los costes administrativos.
4. Obligatoriamente se le deberá contestar en el plazo de un mes a partir de la recepción de la solicitud. Puede existir prórroga de otros dos meses en atención a la complejidad, así como del número de solicitudes. En caso de dicha dilación, se indicarán los motivos.
5. La persona afectada podrá ponerse en contacto con la persona designada como Delegado de Protección de Datos: protecciondedatossepides@sepides.es para solicitar información y con carácter previo a acudir a la AEPD, por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del RGPD.
6. La persona afectada tendrá derecho a presentar una reclamación ante la autoridad de control, en caso de no haber sido atendida su solicitud de ejercicio de derecho, siempre que hubiera transcurrido el plazo que tiene el responsable para contestar o en caso de no estar conforme con la respuesta recibida por el responsable del tratamiento, aportando en la reclamación una copia de la misma.

## II. Derecho de acceso

1. Se le facilitará la siguiente información:
    a. Copia de sus datos personales objeto de tratamiento.
    b. Los fines del tratamiento, así como las categorías de datos personales que se traten.
    c. Los destinatarios o categorías de destinatarios a los que se han comunicado sus datos personales, o serán comunicados, incluyendo en su caso, destinatarios en terceros u organizaciones internacionales.
    d. Información sobre las garantías adecuadas relativas a la transferencia de sus datos a un tercer país o a una organización internacional, en su caso.
    e. El plazo previsto de conservación, o de no ser posible, los criterios para determinar ese plazo.
    f. Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.
    g. Si mis datos personales no se han obtenido directamente de la persona afectada, la información disponible sobre su origen.
    h. La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento.

2. El derecho de acceso, es independiente del derecho de acceso a la información pública que regula la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

### III. Derecho de rectificación

1. El derecho de rectificación se puede ejercitar si los datos personales incluidos en una actividad de tratamiento son inexactos, y deben ser rectificados sin dilación indebida del responsable.
2. Teniendo en cuenta los fines del tratamiento, mediante este derecho se puede solicitar que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.
3. Debe indicar el/los tratamiento/s sobre los que ejercita el derecho de rectificación y la corrección que hay que realizar. Además, cuando sea necesario, deberá acompañarse la solicitud de la documentación que justifique la inexactitud o el carácter incompleto de los datos.

### IV. Derecho de supresión ("derecho al olvido").

1. El derecho al olvido se puede ejercitar cuando concurra alguna de las siguientes circunstancias:
   - Si los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
   - Si el tratamiento de tus datos personales se ha basado en el consentimiento prestó al responsable, y se retira el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime.
   - Si se ha opuesto al tratamiento de tus datos personales al ejercitar el derecho de oposición en las siguientes circunstancias.
   - El tratamiento del responsable se fundamentaba en el interés legítimo o en el cumplimiento de una misión de interés público, y no han prevalecido otros motivos para legitimar el tratamiento de tus datos
   - A que los datos personales sean objeto de mercadotecnia directa, incluyendo la elaboración perfiles relacionada con la citada mercadotecnia.
   - Si los datos personales han sido tratados ilícitamente.
   - Si los datos personales deben 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.
   - Si los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 (condiciones aplicables al tratamiento de datos de los menores en relación con los servicios de la sociedad de la información).
2. El RGPD al regular este derecho lo conecta de cierta forma con el denominado "derecho al olvido", de manera que este derecho de supresión se amplíe de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos.
3. Sin embargo, este derecho no es ilimitado, de tal forma que puede ser factible no proceder a la supresión cuando el tratamiento sea necesario para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, por razones de interés público, en el ámbito de la salud pública, con fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.
4. Debe indicar la identificación el/los tratamiento/s sobre los que ejercita este derecho y las circunstancias señaladas anteriormente aplicables a su caso concreto.

### V. Derecho de oposición

1. El derecho de oposición se puede ejercitar para oponerse a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos
   - Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles, en cuyo caso, el responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

- Cuando el tratamiento tenga como finalidad la mercadotecnia directa, incluida también la elaboración de perfiles anteriormente citada, en cuyo caso, ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines.

2. Debe indicar la identificación el/los tratamiento/s sobre los que ejercita este derecho y las circunstancias señaladas anteriormente aplicables a su caso concreto.

3. Derecho a la limitación del tratamiento

1. El derecho a la limitación del tratamiento consiste en obtener la limitación del tratamiento de los datos que realiza el responsable, si bien su ejercicio presenta dos vertientes:

a. Se puede solicitar la suspensión del tratamiento de los datos:
- Cuando se ha impugnado la exactitud de los datos personales, durante un plazo que permita al responsable su verificación.
- Cuando se ha ejercido el derecho de oposición al tratamiento que el responsable realiza en base al interés legítimo o misión de interés público, mientras aquel verifica si estos motivos prevalecen sobre los del solicitante.

b. Se puede solicitar al responsable la conservación de los datos:
- Cuando el tratamiento sea ilícito y en vez de ejercer el derecho de supresión de los datos, se solicita el derecho de limitación de su uso.
- Cuando 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.

2. Debe indicar la identificación el/los tratamiento/s sobre los que ejercita este derecho y las circunstancias señaladas anteriormente aplicables a su caso concreto y las circunstancias señaladas anteriormente aplicables a su caso concreto.

## VI. Derecho a la portabilidad

1. El derecho a la portabilidad se puede ejercer para recibir los datos personales de un responsable en un formato estructurado, de uso común, de lectura mecánica e interoperable, que permita transmitirlos a otro responsable de tratamiento, siempre que el tratamiento se legitime en base al consentimiento o en el marco de la ejecución de un contrato.

2. No obstante, este derecho, por su propia naturaleza, no se puede aplicar cuando el tratamiento sea necesario para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable o en caso de existir una obligación legal.

3. Debe indicar la identificación el/los tratamiento/s sobre los que ejercita este derecho.

## VII. Derecho a no ser objeto de decisiones individuales automatizadas

1. Este derecho garantiza a los titulares de datos personales que no sean objeto de una decisión basada únicamente en el tratamiento de datos, incluida la elaboración de perfiles, que pueda produzca efectos jurídicos.

2. Se considera elaboración de perfiles, cualquier forma de tratamiento de los datos personales que evalúe aspectos personales que permita, en particular, analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento.

3. Este derecho no será aplicable cuando

- Sea necesario para la celebración o ejecución de un contrato entre el titular de los datos y responsable
- El tratamiento de los datos se fundamente en el consentimiento prestado previamente
- El tratamiento esté autorizado por el Derecho de la Unión o de los Estados miembros y se establezcan medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos del interesado.

Todo ello, sin perjuicio de que el responsable debe garantizar el derecho a obtener la intervención humana, expresar el punto de vista del interesado y la posibilidad de impugnar la decisión. Por otra parte, las excepciones citadas no se aplican con carácter general sobre las categorías especiales de datos.

Debe indicar la identificación el/los tratamiento/s sobre los que ejercita este derecho