

# PROTOCOLO DE SEGURIDAD DE MÍA Y LÍA, S.L.U.

Documento adaptado a las exigencias del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018 de  
Protección de Datos Personales y Garantía de los Derechos Digitales





## Contenido

|        |  |    |
|--------|--|----|
| 1.     | DATOS IDENTIFICATIVOS.....   | 5  |
| 2.     | OBJETO.....  | 5  |
| 3.     | ÁMBITO DE APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD.....  | 7  |
| 4.     | REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO EN LA ORGANIZACIÓN.....   | 11 |
| 5.     | SEGURIDAD DE LA INFORMACIÓN EN LA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES.....  | 26 |
| 6.     | CÓDIGOS DE CONDUCTA EN MATERIA DE PROTECCIÓN DE DATOS. ....  | 30 |
| 7.     | MECANISMOS DE CERTIFICACIÓN EN MATERIA DE PROTECCIÓN DE DATOS. ....  | 30 |
| 8.     | ACTIVOS Y APLICACIONES INFORMÁTICAS. ....  | 31 |
| 9.     | ANÁLISIS DE RIESGOS.....   | 31 |
| 9.1    | ANÁLISIS BÁSICO DE PROTECCIÓN DE DATOS. ....   | 31 |
| 9.1.1  | CUADRO DE ANÁLISIS DE RIESGOS. ....  | 31 |
| 9.1.2  | DESCRIPCIÓN DE FLUJOS DE INFORMACIÓN: CICLO DE VIDA DE LOS DATOS....   | 35 |
| 9.2    | IDENTIFICACIÓN DE LOS RIESGOS.....   | 37 |
| 9.3    | GESTIÓN DE LOS RIESGOS IDENTIFICADOS. ....   | 41 |
| 10.    | MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS ADECUADAS AL RIESGO PARA LOS DATOS OBJETO DE TRATAMIENTO EN LA ORGANIZACIÓN. ....  | 51 |
| 10.1   | SEUDONIMIZACIÓN.....   | 51 |
| 10.2   | CIFRADO DE DATOS PERSONALES.....   | 52 |
| 10.3   | MEDIDAS DE SEGURIDAD QUE GARANTIZAN LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA PERMANENTES DE LOS SISTEMAS Y SERVICIOS DE TRATAMIENTO EN LA ENTIDAD. .... | 52 |
| 10.3.1 | IDENTIFICACIÓN Y AUTENTICACIÓN. USUARIOS AUTORIZADOS. ....   | 52 |
| 10.3.2 | FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS. ....  | 53 |
| 10.3.3 | ACCESOS REMOTOS.....   | 54 |
| 10.3.4 | TRABAJO CON ACCESO DE DATOS PERSONALES FUERA DE LAS INSTALACIONES DE LA ENTIDAD. ....  | 54 |
| 10.3.5 | ENCARGADOS DE LOS TRATAMIENTOS. ....   | 54 |
| 10.3.6 | COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN. CUMPLIMIENTO DEL ART. 32.1.C) DEL RGPD. ....   | 55 |
| 10.3.7 | SOPORTES Y DOCUMENTACIÓN CON DATOS PERSONALES.....   | 55 |
| 10.3.8 | INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD. ....  | 57 |
| 10.4   | PROCESOS Y PROCEDIMIENTOS DE VERIFICACIÓN, EVALUACIÓN Y VALORACIÓN DE LA EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS. ....  | 62 |
| 10.5   | OTRAS MEDIDAS DE SEGURIDAD ADICIONALES. ....   | 63 |
| 11.    | NECESIDAD DE NOMBRAMIENTO DE DELEGADO DE PROTECCIÓN DE DATOS.....  | 63 |

|   |           |
|---|-----------|
| <b>12. MODELOS DE DOCUMENTACIÓN PARA EL EJERCICIO DE LOS DERECHOS POR PARTE DE LOS INTERESADOS.....</b> | <b>65</b> |
| <b>12.1 MODELO DE EJERCICIO DEL DERECHO DE ACCESO.....</b>  | <b>65</b> |
| <b>12.2 MODELO DE EJERCICIO DEL DERECHO DE PORTABILIDAD.....</b>  | <b>66</b> |
| <b>12.3 MODELO DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN.....</b>                                       | <b>66</b> |
| <b>12.4 MODELO DE EJERCICIO DEL DERECHO DE OPOSICIÓN.....</b>   | <b>67</b> |
| <b>12.5 MODELO DE EJERCICIO DEL DERECHO DE SUPRESIÓN (“AL OLVIDO”).....</b>                             | <b>67</b> |
| <b>12.6 MODELO DE EJERCICIO DEL DERECHO DE LIMITACIÓN DEL TRATAMIENTO.....</b>                          | <b>68</b> |
| <b>13. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD.....</b>   | <b>69</b> |



## 1. DATOS IDENTIFICATIVOS.

**Versión: 3.0**

**Protocolo aplicable desde: 15/06/2021.**

|                             |                                       |
|-----------------------------|---------------------------------------|
| <b>Denominación:</b>        | MÍA Y LÍA, S.L.U.                     |
| <b>N.I.F.:</b>              | B70423355                             |
| <b>Inscripción R.M.:</b>    | TOMO: 3527, FOLIO: 160, HOJA: C-51613 |
| <b>Domicilio:</b>           | C/ Real, 105 Bajo (15402 Ferrol)      |
| <b>Correo electrónico:</b>  | administracion@miaylia.com            |
| <b>Sitio web:</b>           | www.miaylia.com                       |
| <b>Actividad principal:</b> | Venta al por menor de ropa infantil   |

### **Figuras con competencia en la seguridad de la información:**

|   | <b>Identificación</b>   |
|---|-------------------------|
| <b>Responsable de la redacción del protocolo de seguridad</b> | ACADEMIA A MARIÑA, S.L. |
| <b>Responsable de los sistemas informáticos</b>               |                         |
| <b>Delegado de protección de datos (DPD)</b>                  | NO PROCEDE              |

## 2. OBJETO.

El Diario Oficial de la Unión Europea publicó el 4 de mayo de 2016 el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).

La seguridad se establece en el RGPD como un principio, según determina su artículo 5, además de como una obligación, desarrollada en el Capítulo IV, Sección 2 del mismo texto normativo.

El Considerando (39) del RGPD señala que los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas, incluyendo el impedimento de accesos o usos no autorizados de los datos y del equipo utilizado en el tratamiento.

En similar sentido, y de forma muy general, se recoge en el artículo 5.1.f) bajo el epígrafe “Principios relativos al tratamiento”. Se dice en este precepto, que los datos personales deben ser “tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (<<integridad y confidencialidad>>”).

El mismo RGPD, en su artículo 32, referido a la “seguridad del tratamiento”, determina una serie de medidas técnicas y organizativas que deben implementarse como mínimo. Señala este precepto, en su apartado 1º, que “teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros.”

- La seudonimización. El Reglamento General, en su artículo 4.5, señala que seudonimización es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

- El cifrado de datos personales. En el artículo 6.4 e) del RGPD se indica que en el caso de que el responsable o el encargado realicen un tratamiento de datos para un fin distinto a aquel para el que se recogieron, o bien no se cuenta con el consentimiento del mismo, o no existe una habilitación normativa que justifique dicho tratamiento, deberán tener en cuenta (potestativo) “la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización”. El Considerando (83) del RGPD indica que “a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado”.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento:
  - Confidencialidad implica que la información únicamente debe ser accesible o divulgada a aquellos que están autorizados.
  - La integridad supone que la información debe permanecer correcta (integridad de los datos) y como el emisor la originó (integridad de fuentes), sin que quepa la manipulación por terceros.
  - La disponibilidad implica que la información debe estar permanentemente accesible para aquellos que estén autorizados.
  - La resiliencia (en inglés, *resilience*) en sistemas tecnológicos, se define como la capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones. La RAE define resiliencia como “la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido”.
- 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.

El RGPD no hace referencia alguna a la necesidad de mantener un “documento de seguridad” como se venía conociendo hasta ahora; si bien, sí que se exige, en el artículo 30, la necesidad de mantener un “registro de las actividades de tratamiento”, donde entre otras cuestiones se describa, de forma general y potestativa, las medidas técnicas y organizativas de seguridad a la que se refiere el artículo 32, apartado 1 del RGPD. Señala el artículo 30.1 que “cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener (...) g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1”.

Se puede acreditar el cumplimiento de estas medidas de seguridad (artículo 32.3 RGPD) si el responsable o el encargado se han adherido a:

- Un código de conducta (aprobado según fija el artículo 40 RGPD).
- Un mecanismo de certificación (aprobado a tenor del artículo 42 RGPD).

En los artículos 33 y 34 del RGPD se contemplan previsiones relativas a la notificación de violaciones de seguridad de los datos a la autoridad de control y al interesado, que serán analizadas posteriormente.

Finalmente, el RGPD en su artículo 32.4 determina que el responsable y el encargado del tratamiento deben tomar medidas para garantizar que cualquier persona que actúe bajo su autoridad y tengan acceso a datos personales únicamente pueden tratar dichos datos siguiendo instrucciones del responsable, salvo que una norma señale lo contrario.

Por todo ello, el presente Protocolo y Política de Seguridad recoge las medidas técnicas y organizativas necesarias para garantizar en la entidad la protección, confidencialidad, integridad, disponibilidad y resiliencia de los recursos.

El presente protocolo se deberá mantener en todo momento actualizado, y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en la organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados.

Del mismo modo, será objeto de revisión si se producen cambios en la normativa sobre protección de datos de carácter personal, o se modifican los criterios establecidos por las Autoridades Europeas de Protección de Datos o la AEPD, a través de sus Informes, Recomendaciones o Resoluciones, y en todo caso como consecuencia de Sentencias del Tribunal de Justicia de la UE; la Audiencia Nacional, Tribunal Supremo, o Tribunal Constitucional.

### 3. ÁMBITO DE APLICACIÓN DE LAS MEDIDAS DE SEGURIDAD.

El presente protocolo de seguridad será de aplicación y vinculará a los ficheros que contengan datos de carácter personal que se encuentren bajo responsabilidad de la entidad en cuestión, así como a los sistemas de información operantes, soportes y equipos empleados para el tratamiento de los datos que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, además de a las personas que intervengan en el tratamiento de los mismos y a los establecimientos, locales y otros lugares afectados por ello:

| INSTALACIONES     | DOMICILIO                        |
|-------------------|----------------------------------|
| MÍA Y LÍA, S.L.U. | C/ Real, 105 Bajo (15402 Ferrol) |

El presente protocolo de seguridad es de obligado cumplimiento para todo el personal de la organización con acceso a datos personales (se encuentren o no automatizados) o a los sistemas de información que permitan el acceso a los mismos. A tal fin, todo empleado suscribe el protocolo con obligaciones de seguridad que incluye cláusulas de confidencialidad de la información a la que tienen acceso en el desempeño de su actividad.

| OBLIGACIONES DE SEGURIDAD DE LA ENTIDAD               |                   |                                   |
|---|-------------------|-----------------------------------|
| VERSIÓN DEL PROTOCOLO DE SEGURIDAD Y CONFIDENCIALIDAD | FECHA DE CREACIÓN | FECHA DE ACTUALIZACIÓN O REVISIÓN |
| VERSIÓN 1.0   | 23/08/2018        |                                   |
| VERSIÓN 2.0   | 24/09/2019        |                                   |
| VERSIÓN 3.0   | 15/06/2021        |                                   |
|   |                   |                                   |

El presente protocolo de seguridad se aplica tanto a los ficheros automatizados como a los que se encuentran en soporte papel, al centro de tratamiento, equipos informáticos, sistemas, programas, soportes y otros medios o herramientas, como a las personas que intervengan en el tratamiento de los datos de carácter personal, garantizado así los niveles de seguridad exigidos legalmente.

Tanto la estructura de cada uno de los ficheros como los lugares, el servidor y el entorno del sistema operativo y de comunicaciones en los que se encuentran ubicados tales ficheros, se detallan a continuación:

| <b>Identificación del Fichero</b>   |
|---|
| <b>FICHERO “CLIENTES, USUARIOS Y OTROS INTERESADOS”</b>   |
| <b>Tipología de datos tratados</b>  |
| Datos de clientes, usuarios, solicitantes de servicios, potenciales clientes y usuarios, representantes legales y otros:<br>Nombre y apellidos, DNI/NIF/NIE/documento identificativo, nacionalidad, edad, fecha de nacimiento y otras características personales, domicilio, dirección de correo electrónico, teléfono, datos bancarios, económicos, financieros y de seguros, datos comerciales y de servicios, posibles datos de sonidos y voz, posibles imágenes, firma, posible firma digital y/o digitalizada y, en su caso, posibles categorías especiales.   |
| <b>Tratamiento Automatizado/Manual/Mixto</b>  |
| MIXTO   |
| <b>Estructura</b>   |
| En el fichero de “CLIENTES, USUARIOS Y OTROS INTERESADOS” se lleva a cabo tanto tratamiento automatizado como tratamiento no automatizado.<br>Para el tratamiento automatizado se utilizan 5 ordenadores de sobremesa, equipados con sistema operativo Windows, y 1 TPV.<br>El programa utilizado para la gestión de la información es POWER SHOP, comercializado por POWER SOLUTIONS, S.L., además del paquete de ofimática.<br>El fichero “CLIENTES, USUARIOS Y OTROS INTERESADOS” es también objeto de tratamiento no automatizado. La documentación referente a este fichero se guarda en un archivador que cuenta con acceso restringido, al igual que el local donde se encuentra ubicado.<br>En todos los casos, para la documentación en soporte papel que deba ser desechada, el proceso de destrucción se debería realizar siempre mediante destructora de papel. |
| <b>Descripción del entorno</b>  |
| El fichero se encuentra, tanto en su parte automatizada como en su parte manual, guardado en las instalaciones de MÍA Y LÍA, S.L.U. Dicho local cuenta con acceso restringido mediante cerradura, y, en lo referente al acceso automatizado, solo podrán acceder aquellos usuarios autorizados en el presente documento.  |

| <b>Identificación del Fichero</b>   |
|---|
| <b>FICHERO “PROVEEDORES”</b>  |
| <b>Tipología de datos tratados</b>  |
| Datos de proveedores, potenciales proveedores y/o representantes legales (en cuestiones relativas a personas físicas):<br>Nombre, apellidos y otros datos identificativos, DNI/NIF/NIE/documento identificativo, domicilio, dirección correo electrónico, teléfono, datos bancarios, económicos, financieros y de seguros, datos comerciales y de servicios, posibles datos de sonidos y voz, posibles imágenes, firma, posible firma digital y/o digitalizada y otros. |
| <b>Tratamiento Automatizado/Manual/Mixto</b>  |
| MIXTO   |
| <b>Estructura</b>   |
| En el fichero de “PROVEEDORES” se lleva a cabo tanto tratamiento automatizado como tratamiento no automatizado.   |

Para el tratamiento automatizado se utilizan 5 ordenadores de sobremesa, equipados con sistema operativo Windows.

El programa utilizado para la gestión de la información es el paquete de ofimática.

El fichero "PROVEEDORES" es también objeto de tratamiento no automatizado. La documentación referente a este fichero se guarda en un archivador que cuenta con acceso restringido, al igual que el local donde se encuentra ubicado.

En todos los casos, para la documentación en soporte papel que deba ser desechada, el proceso de destrucción se debería realizar siempre mediante destructora de papel.

**Descripción del entorno**

El fichero se encuentra, tanto en su parte automatizada como en su parte manual, guardado en las instalaciones de MÍA Y LÍA, S.L.U. Dicho local cuenta con acceso restringido mediante cerradura, y, en lo referente al acceso automatizado, solo podrán acceder aquellos usuarios autorizados en el presente documento.

**Identificación del Fichero**

**FICHERO "NÓMINAS, PERSONAL Y RECURSOS HUMANOS"**

**Tipología de datos tratados**

Datos de candidatos, posible personal (laboral, societario, voluntariado, becarios, colaboradores, autónomos y otros posibles), familiares y/o representantes legales y sindicales (en su caso):

Nombre y apellidos, DNI/NIF/NIE/documento identificativo, nacionalidad, sexo, fecha de nacimiento, domicilio, teléfono, datos bancarios, económicos, financieros y de seguros, CV, titulaciones y otra documentación acreditativa de estudios cursados, vida laboral, formación, experiencia profesional, parte de bajas y altas, datos de nómina, Seguridad Social, mutualidad, firma, posible firma digital y/o digitalizada, afiliación sindical (en su caso), datos académicos y profesionales, copia de sanciones en el ámbito de la entidad si procediese, posibles datos de sonidos y voz, posibles imágenes, posibles categorías especiales y otros (véase el RAT "gestión de recursos humanos").

**Tratamiento Automatizado/Manual/Mixto**

MIXTO

**Estructura**

El fichero "NÓMINAS, PERSONAL Y RECURSOS HUMANOS" es objeto de tratamiento automatizado y no automatizado.

Para el tratamiento automatizado se utilizan 5 ordenadores de sobremesa, equipados con sistema operativo Windows.

El programa utilizado para la gestión de la información es el paquete de ofimática.

El fichero "NÓMINAS, PERSONAL Y RECURSOS HUMANOS" es también objeto de tratamiento no automatizado. La documentación referente a este fichero se guarda en un archivador que cuenta con acceso restringido, al igual que el local donde se encuentra ubicado.

En todos los casos, para la documentación en soporte papel que deba ser desechada, el proceso de destrucción se debería realizar siempre mediante destructora de papel.

**Descripción del entorno**

El fichero se encuentra, tanto en su parte automatizada como en su parte manual, guardado en las instalaciones de MÍA Y LÍA, S.L.U. Dicho local cuenta con acceso restringido mediante cerradura, y, en lo referente al acceso automatizado, solo podrán acceder aquellos usuarios autorizados en el presente documento.

| <b>Identificación del Fichero</b>  |
|--|
| <b>FICHERO “CONTROL DE ACCESO A LAS INSTALACIONES Y REGISTRO”</b>  |
| <b>Tipología de datos tratados</b>   |
| Datos identificativos del sujeto:<br>Nombre, apellidos, DNI/NIF/NIE/documento identificativo, datos de control de presencia (fecha/hora entrada y salida, motivo de ausencia), posible verificación/autenticación biométrica, posibles datos de sonidos y voz, firma y posible firma digital y/o digitalizada y otros posibles datos identificativos.  |
| <b>Tratamiento Automatizado/Manual/Mixto</b>   |
| MANUAL   |
| <b>Estructura</b>  |
| El fichero de “CONTROL DE ACCESO A LAS INSTALACIONES Y REGISTRO” es objeto de tratamiento manual únicamente.<br>El fichero consiste en hojas de firma donde quedan registrados los accesos a las instalaciones. La documentación referente a este fichero se guarda en un archivador que cuenta con acceso restringido al igual que el local donde se encuentra ubicado.<br>En todos los casos, para la documentación en soporte papel que deba ser desechada, el proceso de destrucción se debería realizar siempre mediante el empleo de destructora de papel. |
| <b>Descripción del entorno</b>   |
| El fichero se encuentra organizado en toda su extensión en soporte manual y guardado en las instalaciones de MÍA Y LÍA, S.L.U. Dicho local cuenta con acceso restringido mediante cerradura.   |

| <b>Identificación del Fichero</b>   |
|---|
| <b>FICHERO “USUARIOS WEB Y OTRAS PLATAFORMAS Y APLICACIONES”</b>  |
| <b>Tipología de datos tratados</b>  |
| Datos identificativos del sujeto:<br>Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, domicilio, datos de características personales, bancarios, económicos y financieros, datos comerciales y de servicios, correo electrónico, teléfono y dirección IP, posibles datos de sonidos y voz, posibles imágenes, posibles cookies y otros.  |
| <b>Tratamiento Automatizado/manual/Mixto</b>  |
| AUTOMATIZADO  |
| <b>Estructura</b>   |
| El fichero de “USUARIOS WEB Y OTRAS PLATAFORMAS Y APLICACIONES” se lleva a cabo mediante tratamiento automatizado.<br>Para el tratamiento automatizado se utilizan 5 ordenadores de sobremesa, equipados con sistema operativo Windows, y el teléfono móvil.<br>El tratamiento de los datos de los usuarios de la web, se lleva a cabo mediante el empleo de navegadores web y del paquete de ofimática; los datos de los usuarios de las redes sociales se manejan desde las aplicaciones contenidas en el software de Facebook e Instagram. |

| Descripción del entorno  |
|--|
| La parte del fichero que comprende los datos de los usuarios de la web se guarda en las instalaciones y servidores de MÍA Y LÍA, S.L.U., mientras que los datos de los usuarios de las redes sociales están en los servidores de Facebook e Instagram. Todos ellos observan las medidas de seguridad correspondientes. |

#### 4. REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO EN LA ORGANIZACIÓN.

A continuación, se recoge el registro de las actividades de tratamiento (artículo 30.1 del RGPD) que es actuante para la presente entidad, donde entre otras cuestiones se describe, de forma general y potestativa, las medidas técnicas y organizativas de seguridad. Además, se contemplará la realización de un registro de categorías de actividades de tratamiento, efectuadas por cuenta de un hipotético responsable si, en su caso, se ostentase en algún supuesto la condición de encargado del tratamiento (artículo 30.2 del RGPD). Este último registro de categorías será anexado como agregado apartado en el registro de cada actividad de tratamiento existente. Ello para ser cumplimentado en caso de pertinencia si se da tal situación.

A mayores, tanto el registro de actividades como de categorías deberá ser actualizado en caso de sufrir novedades; tanto por agregación de nuevas actividades de tratamiento o categorías en situación de encargado, como por baja de alguna de estas.

Por otro lado, en cuanto a las medidas de seguridad operantes, se tendrá en consideración tanto las específicamente contempladas en cada registro particular como las restantes previstas en este protocolo.

Por último, a título ilustrativo y con opción de desarrollo, se tiene presente la existencia de los modelos recogidos en la *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, de la AEPD. Ello en cuanto al Anexo IV y V sobre plantillas para el registro de actividades de tratamiento del responsable y del encargado respectivamente: <https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf>

| REGISTRO DE ACTIVIDADES EN LA ENTIDAD MÍA Y LÍA, S.L.U.                            |   |   |
|--|---|---|
| <b>La obligación del mantenimiento del registro de actividades se deriva de:</b>   | Entidad que emplea más de 250 personas.                                 |   |
|  | Se realizan tratamientos con riesgo.                                    |   |
|  | Tratamiento no ocasional ( <i>determinado preventivamente</i> ).        | X |
|  | Se realizan tratamientos con categorías especiales de datos personales. |   |
|  | Se realizan tratamientos relativos a condenas de infracciones penales.  |   |
| <b>Formato en el que se mantiene el registro y posibles agentes intervinientes</b> | En soporte papel.   | X |
|  | En soporte electrónico.   | X |
|  | Corresponsables, representantes y otros.                                |   |
|  | Delegado de Protección de Datos.  |   |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE CLIENTES, USUARIOS Y OTROS INTERESADOS.</b>                 |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.a): Consentimiento específico.<br>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.<br>RGPD: 6.1.c): Obligación legal.<br>RGPD: 6.1.f): Intereses legítimos.<br>RGPD: 9.2 |
| <b>FINES DEL TRATAMIENTO</b>   | Prestación del servicio contractualmente acordado.<br>Gestión administrativa.<br>Asesoramiento solicitado.<br>Atención de solicitudes y consultas.<br>Posible gestión de encuestas, estudios, quejas y sugerencias, etc.<br>Actividades informativas, comerciales o de promoción con habilitación para ello.<br>Otras finalidades.  |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Clientes, usuarios, solicitantes de servicios, potenciales clientes y usuarios, representantes legales y otros.   |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, edad, fecha de nacimiento y otras características personales, dirección y domicilio, correo electrónico, datos bancarios, económicos, financieros y de seguros, datos comerciales y de servicios, firma, datos de contacto, posible firma digital y/o digitalizada, posibles datos de sonidos y voz, posibles imágenes y, en su caso, posibles categorías especiales.               |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>   | Administración tributaria.<br>Entidades financieras.<br>Bancos, cajas de ahorros y cajas rurales.<br>Servicios auxiliares para el cumplimiento contractual.<br>Otras cesiones por obligación legal, ejecución contractual, intereses legítimos o con consentimiento válidamente otorgado por parte del afectado.  |
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.   |

|  |  |
|--|--|
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | 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 del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD. |
| <b>MEDIDAS DE SEGURIDAD:</b>   |  |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |  |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |  |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |  |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |  |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |  |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |  |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |  |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente Documento.   |  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |  |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>  |  |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.   |  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>   |  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.  |  |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE USUARIOS WEB Y OTRAS PLATAFORMAS Y APLICACIONES.</b>        |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.a): El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. |

|  |   |
|--|---|
|  | <p>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.</p> <p>RGPD: 6.1.c): Obligación legal.</p> <p>RGPD: 6.1.f): Intereses legítimos.</p> <p>RGPD: 9.2</p> <p>La Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).-</p> |
| <b>FINES DEL TRATAMIENTO</b>   | Gestión de servicio y atención a consultas planteadas a través del sitio web u otras plataformas digitales, programas, aplicaciones, etc. y acciones informativas, comerciales o promocionales con habilitación para ello. Posible gestión de encuestas, estudios, quejas y sugerencias, etc. Gestión administrativa. Otras finalidades.  |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Usuarios web y de otras plataformas digitales, programas, aplicaciones etc.   |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, DNI/NIF/NIE/documento identificativo, nacionalidad, dirección y domicilio, teléfono, correo electrónico, datos de características personales, bancarios, económicos y financieros, datos comerciales y de servicios, posibles datos de sonidos y voz, posibles imágenes, dirección IP, posibles cookies y otros.  |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>   | No están previstas cesiones de datos salvo por cumplimiento legal, ejecución contractual, intereses legítimos, o con consentimiento válidamente otorgado por parte del afectado.  |
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.   |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | 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 del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD.                              |
| <b>MEDIDAS DE SEGURIDAD:</b>   |   |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |   |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |   |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |   |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |   |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |   |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |   |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |   |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.   |   |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |   |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |   |

|   |
|---|
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>   |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.                        |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo. |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE ACCESO A LAS INSTALACIONES Y REGISTRO.</b>                  |  |
|--|--|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.  |
| <b>DPD</b>   | NO PROCEDE   |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:  |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):   |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.a): El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.<br>RGPD: 6.1.b): Ejecución contractual.<br>RGPD: 6.1.c): Obligación legal.<br>RGPD: 6.1.f): El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. |
| <b>FINES DEL TRATAMIENTO</b>   | Control de acceso a las instalaciones (y registro de la jornada laboral, en su caso) en cuanto al personal de la entidad o, si procede, terceros ajenos a la misma.  |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Clientes, trabajadores, representantes legales, solicitantes de servicios, proveedores.<br>Terceros que acceden a la información.<br>Otros.  |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, dirección y domicilio, correo electrónico, teléfono, datos de control de presencia (fecha/hora entrada y salida, motivo de ausencia), firma, posible firma digital y/o digitalizada, posibles datos de sonidos y voz, posible verificación/autenticación biométrica y otros posibles datos identificativos.  |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>   | No están previstas cesiones de datos salvo obligación legal.   |

|  |  |
|--|--|
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.  |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | 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 del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD. |
| <b>MEDIDAS DE SEGURIDAD:</b>   |  |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |  |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |  |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |  |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |  |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |  |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |  |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |  |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.   |  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |  |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>  |  |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.   |  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>   |  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.  |  |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE PROVEEDORES.</b>  |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.a): El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. |

|   |   |
|---|---|
|   | <p>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.</p> <p>RGPD: 6.1.c): Obligación legal.</p> <p>RGPD: 6.1.f): Intereses legítimos.</p> <p>Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil.-</p>      |
| <b>FINES DEL TRATAMIENTO</b>  | <p>Gestión integral de la relación mantenida con los proveedores o potenciales proveedores en cuanto a la dación del servicio, acciones informativas o para el oportuno cumplimiento legal.</p> <p>Gestión administrativa.</p>  |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>  | <p>Proveedores, potenciales proveedores y/o representantes legales (en cuestiones relativas a personas físicas).</p>  |
| <b>CATEGORÍAS DE DATOS</b>  | <p>Nombre, apellidos y otros datos identificativos, DNI/NIF/NIE/documento identificativo, teléfono, correo electrónico, domicilio, mail, fax, datos bancarios, económicos, financieros y de seguros, datos comerciales y de servicios, firma, posible firma digital y/o digitalizada, posibles imágenes, posibles datos de sonidos y voz y otros.</p>                               |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>  | <p>Administración tributaria.</p> <p>Entidades bancarias y financieras.</p> <p>Cajas de ahorro.</p> <p>Cajas rurales.</p> <p>Servicios auxiliares para el cumplimiento contractual.</p> <p>Otras administraciones.</p> <p>Otras comunicaciones por obligación legal, ejecución contractual o intereses legítimos.</p>   |
| <b>TRANSFERENCIAS INTERNACIONALES</b>   | <p>No están previstas transferencias internacionales de los datos.</p>  |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>  | <p>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 del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD.</p> |
| <b>MEDIDAS DE SEGURIDAD:</b>  |   |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>  |   |
| <p>En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.</p>   |   |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>  |   |
| <p>Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes.</p> |   |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>   |   |
| <p>Se debe atender a lo dispuesto en el apartado 8 del presente documento.</p>  |   |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>   |   |
| <p>Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.</p>   |   |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>  |   |

|   |
|---|
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas. |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>   |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.                                 |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN CONTABLE, TRIBUTARIA Y PRESUPUESTARIA.</b>                     |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de datos.-<br>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato.<br>RGPD: 6.1.c): Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.<br>Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.-<br>Ley 58/2003, de 17 de diciembre, General Tributaria.-<br>Ley 38/2003, de 17 de noviembre, General de Subvenciones.- |
| <b>FINES DEL TRATAMIENTO</b>   | Tramitación de expedientes de gastos e ingresos derivados de la ejecución del presupuesto de la entidad y su actividad mercantil. Ello además del cumplimiento de las previsiones tributarias. Gestión administrativa.  |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Clientes, proveedores, personal.  |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, dirección y domicilio, firma, posible firma digital y/o digitalizada, correo electrónico y teléfono.<br>Datos de detalle de empleo: puesto de trabajo.<br>Datos contables, tributarios, fiscales, presupuestarios, bancarios, económico-financieros y de seguros.   |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>   | Entidades bancarias y financieras.<br>Instituto Nacional de la Seguridad Social y mutualidades.<br>Agencia Estatal de Administración Tributaria.<br>Intervención General de la Administración del Estado.<br>Otras cesiones por obligación legal, ejecución contractual o intereses legítimos.  |

|  |  |
|--|--|
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.  |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | 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 del tratamiento de vinculado a tal finalidad, y conforme a la Ley 58/2003, de 17 de diciembre, General Tributaria, además de los periodos establecidos en agregada legislación. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD. |
| <b>MEDIDAS DE SEGURIDAD:</b>   |  |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |  |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |  |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |  |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |  |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |  |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |  |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |  |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.   |  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |  |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>  |  |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.   |  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>   |  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.  |  |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE RECURSOS HUMANOS.</b>                                       |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de datos.-<br>RGPD: 6.1.a): El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. |

|   |  |
|---|--|
|   | <p>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.</p> <p>RGPD: 6.1.c): Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.</p> <p>RGPD: 6.1.f): Intereses legítimos.</p> <p>Otros posibles supuestos del art. 6.1 del RGPD.</p> <p>RGPD: 9.2 (condicionado por el art. 9.1 de la LOPDGDD).</p> <p>Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.-</p> <p>Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de hombres y mujeres.-</p> <p>Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales.</p>  |
| <p><b>FINES DEL TRATAMIENTO</b></p>                         | <p>Selección, formación y gestión del posible personal, destinado en MÍA Y LÍA, S.L.U.</p> <p>Expediente personal. Control horario. Incompatibilidades. Formación. Gestión de nómina. Planes de pensiones. Acción social. Prevención de riesgos laborales. Posible régimen disciplinario. Gestión de posibles protocolos de acoso sexual, acoso por razón de sexo y materias vinculadas.</p> <p>Emisión de la nómina del personal de la entidad, así como de todos los productos derivados de la misma.</p> <p>Gestión económica de la acción social y obtención de estudios estadísticos o monográficos destinados a la gestión económica del personal.</p> <p>Atención de solicitudes, reclamaciones, derechos y otros.</p> <p>Gestión de la actividad sindical.</p>   |
| <p><b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b></p> | <p>Candidatos y posible personal destinado en la entidad (laboral, societario, voluntariado, becarios, colaboradores, autónomos y otros posibles) y sus familiares, así como representantes legales y/o sindicales en su caso.</p>   |
| <p><b>CATEGORÍAS DE DATOS</b></p>                           | <p>Nombre y apellidos, nacionalidad, dirección y domicilio, DNI/NIF/NIE/documento identificativo, número de registro de personal (en su caso), datos de la Seguridad Social, mutualidad, dirección, firma, posible firma digital y/o digitalizada, datos bancarios, económicos, financieros y de seguros, teléfono, correo electrónico, posibles imágenes, posibles datos de sonidos y voz y otros posibles datos identificativos.</p> <p>Categorías especiales de datos (posibles): datos de salud (bajas por enfermedad, accidentes laborales y grado de discapacidad, sin inclusión de diagnósticos), afiliación sindical (en su caso), a los exclusivos efectos de pago de cuotas sindicales (en su caso), representante sindical (en su caso), justificantes de asistencia de propios y de terceros y otros.</p> <p>Datos de características personales (posibles): Sexo, estado civil, nacionalidad, edad, fecha y lugar de nacimiento y datos de características y circunstancias familiares: Fecha de alta y baja, licencias, permisos y autorizaciones.</p> |

|  |  |
|--|--|
|  | <p>Datos académicos y profesionales (posibles): CV, recomendaciones y referencias, titulaciones y otra documentación acreditativa de estudios cursados, vida laboral, formación y experiencia profesional.</p> <p>Datos de detalle de empleo. Incompatibilidades.</p> <p>Datos de control de presencia: fecha/hora entrada y salida, motivo de ausencia, datos de ubicación.</p> <p>Datos económico-financieros (posibles): Datos económicos de nómina, créditos, préstamos, avales, deducciones impositivas baja de haberes correspondiente al puesto de trabajo anterior (en su caso), retenciones judiciales (en su caso), otras retenciones (en su caso). Datos bancarios.</p> <p>Otros datos (posibles): datos relativos a la acción social, datos sobre sanciones en materia de función pública.</p> |
| <b>DESTINATARIOS:<br/>CESIONES PREVISTAS</b>   | <p>Entidades a quienes se le encomienden la gestión en materia de prevención de riesgos laborales (en supuestos de comunicación, no de acceso a datos).</p> <p>Instituto Nacional de la Seguridad Social.</p> <p>Mutuas y otras entidades de vigilancia de la salud.</p> <p>Tesorería General de la Seguridad Social.</p> <p>Organizaciones sindicales (existiendo, en su caso, habilitación específica para ello).</p> <p>Entidades bancarias y financieras.</p> <p>Agencia Estatal de Administración Tributaria.</p> <p>Otras cesiones por obligación legal, consentimiento válidamente otorgado, ejecución contractual, intereses legítimos u otras comunicaciones basadas en otros supuestos habilitadores (pudiéndose ampliar la legitimación de tal tratamiento).</p>                                |
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.  |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | <p>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 del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule.</p> <p>Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD.</p>   |
| <b>MEDIDAS DE SEGURIDAD:</b>   |  |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |  |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |  |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |  |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |  |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |  |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |  |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |  |

|   |
|---|
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas. |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>   |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.                                 |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE AGENDA DE MÍA Y LÍA, S.L.U..</b>                            |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de datos.-<br>RGPD: 6.1.b): Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.<br>RGPD: 6.1.f): El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. |
| <b>FINES DEL TRATAMIENTO</b>   | Esta actividad de tratamiento responde a las relaciones y acciones de comunicación de la entidad. Gestión administrativa.   |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Personas físicas, incluidas las que representan a personas jurídicas, públicas y privadas, con las que la entidad mantiene relación en función de las actividades que tienen encomendadas.  |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, dirección y domicilio, firma, posible firma digital y/o digitalizada, teléfono y correo electrónico.  |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>   | Personas físicas, incluidas las que representan a personas jurídicas relacionadas con las actividades de MÍA Y LÍA, S.L.U. Ello con las habilitaciones legales oportunas.   |

|  |   |
|--|---|
| <b>TRANSFERENCIAS INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.   |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>   | Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron, además de para determinar las posibles responsabilidades que se pudieran derivar del tratamiento vinculado a tal finalidad. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD. |
| <b>MEDIDAS DE SEGURIDAD:</b>   |   |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |   |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |   |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |   |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |   |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |   |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |   |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |   |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.   |   |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |   |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |   |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>  |   |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.   |   |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>   |   |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.  |   |

|  |   |
|--|---|
| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE RECLAMACIONES, INCIDENTES Y OTROS.</b>                      |   |
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.a): El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. |

|   |   |
|---|---|
|   | <p>RGPD: 6.1.c): Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.</p> <p>RGPD: 6.1.f): Intereses legítimos.</p> <p>Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General de Defensa de Usuarios y Consumidores.-</p> <p>Código Civil.-</p>  |
| <b>FINES DEL TRATAMIENTO</b>  | <p>Esta actividad de tratamiento responde a dar cumplido trámite a las distintas solicitudes, acciones de ejercitación de derechos y reclamaciones presentadas por los clientes, usuarios y otros interesados, además de acciones informativas y de gestión administrativa en general. También obedece a la gestión de posibles incidentes y violaciones de la seguridad y posibles actuaciones relativas a la notificación y comunicación del hecho a la AEPD y a los interesados, respectivamente y en su caso. De igual manera, también puede incluir la gestión de consultas previas ante la propia AEPD. Todo ello si afecta al tratamiento de datos personales.</p> |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>  | <p>Personas físicas, incluidos los representantes.</p>  |
| <b>CATEGORÍAS DE DATOS</b>  | <p>Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, dirección y domicilio, firma, datos bancarios, económicos, financieros y de seguros, posibles imágenes, posibles datos de sonidos y voz, posible firma digital y/o digitalizada, teléfono, correo electrónico y otros posibles.</p>  |
| <b>DESTINATARIOS: CESIONES PREVISTAS</b>  | <p>Organismos dedicados al arbitraje judicial.</p> <p>Organismos y administraciones públicas.</p> <p>Tribunales y Juzgados.</p> <p>Entidades aseguradoras y reaseguradoras.</p> <p>AEPD.</p> <p>Personas afectadas.</p> <p>Otras cesiones por obligación legal, intereses legítimos o con consentimiento válidamente otorgado por parte del afectado.</p>   |
| <b>TRANSFERENCIAS INTERNACIONALES</b>   | <p>No están previstas transferencias internacionales de los datos.</p>  |
| <b>PLAZO DE CONSERVACIÓN Y SUPRESIÓN</b>  | <p>Se conservarán durante el tiempo necesario para cumplir con las exigencias derivadas de la presentación de la reclamación y demás finalidades, además de para determinar las posibles responsabilidades que se pudieran derivar del tratamiento vinculado a tales finalidades. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD.</p>  |
| <b>MEDIDAS DE SEGURIDAD:</b>  |   |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>  |   |
| <p>En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.</p>   |   |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>  |   |
| <p>Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes.</p> |   |

|   |
|---|
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>   |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.   |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>   |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas. |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN</b>   |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.                                 |

| <b>REGISTRO DE ACTIVIDADES: GESTIÓN DE IMPAGOS DE CLIENTES Y OTROS.</b>                            |   |
|--|---|
| <b>RESPONSABLE DEL TRATAMIENTO y representante en su caso (datos de contacto en el apartado 1)</b> | MÍA Y LÍA, S.L.U.   |
| <b>DPD</b>   | NO PROCEDE  |
| <b>CORRESPONSABLE (en su caso)</b>   | Nombre y datos de contacto:   |
| <b>SITUACIÓN DE ENCARGADO POR CUENTA DE (en su caso):</b>  | Nombre y representante / datos de contacto / categorías de tratamientos / DPD si lo hubiese (y sus datos de contacto):  |
| <b>BASE JURÍDICA</b>   | Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales.-<br>Reglamento General de Protección de Datos.-<br>RGPD: 6.1.c): Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.<br>RGPD: 6.1.f): El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.<br>Código Civil.- |
| <b>FINES DEL TRATAMIENTO</b>   | Esta actividad de tratamiento responde al interés legítimo del responsable de cobrar los servicios prestados y no pagados.<br>Gestión administrativa.   |
| <b>CATEGORÍAS DE INTERESADOS: COLECTIVO AFECTADO</b>   | Personas físicas, incluidos los representantes legales.   |
| <b>CATEGORÍAS DE DATOS</b>   | Nombre y apellidos, nacionalidad, DNI/NIF/NIE/documento identificativo, dirección y domicilio, datos bancarios, económicos, financieros y de seguros, firma, posible firma digital y/o digitalizada, posibles imágenes, posibles datos de sonidos y voz, teléfono y correo electrónico.   |

|  |  |
|--|--|
| <b>DESTINATARIOS:<br/>CESIONES PREVISTAS</b>   | Organismos dedicados al arbitraje judicial.<br>Tribunales y Juzgados.<br>Otras cesiones por obligación legal e intereses legítimos.  |
| <b>TRANSFERENCIAS<br/>INTERNACIONALES</b>  | No están previstas transferencias internacionales de los datos.  |
| <b>PLAZO DE CONSERVACIÓN<br/>Y SUPRESIÓN</b>   | Se conservarán durante el tiempo necesario para cumplir con las exigencias derivadas de la presentación de la reclamación u otras finalidades, además de para determinar las posibles responsabilidades que se pudieran derivar del tratamiento vinculado a tales finalidades. Siempre teniendo presente el plazo de conservación que legalmente se estipule. A mayores y, en su caso, se dará cumplimiento al art. 32 de la LOPDGD. |
| <b>MEDIDAS DE SEGURIDAD:</b>   |  |
| <b>ACTIVOS Y APLICACIONES INFORMÁTICAS</b>   |  |
| En lo referente al uso de activos y aplicaciones informáticas empleadas para el tratamiento arriba enunciado, se debe estar a lo dispuesto en el apartado 8.   |  |
| <b>GESTIÓN DE SOPORTES Y DOCUMENTACIÓN</b>   |  |
| Los soportes utilizados para el tratamiento de datos de carácter personal deben cumplir las exigencias del apartado 10.3.7 del presente documento, debiendo garantizar en todo momento su integridad y quedando registrado el contenido de los soportes. |  |
| <b>SOPORTES AUTOMATIZADOS Y SISTEMAS DE INFORMACIÓN</b>  |  |
| Se debe atender a lo dispuesto en el apartado 8 del presente documento.  |  |
| <b>EJECUCIÓN DEL TRATAMIENTO FUERA DE LAS INSTALACIONES</b>  |  |
| Deberá constar en todo caso, formulario habilitado al efecto, y cumplir con las exigencias recogidas en el apartado 10.3.4 del presente documento.   |  |
| <b>PROCEDIMIENTO DE IDENTIFICACIÓN</b>   |  |
| Los perfiles de los usuarios autorizados deberán estar incluidos en el cuadro recogido en el apartado 10.3.1 y cumplir las estipulaciones referentes a autenticación y política de contraseñas.  |  |
| <b>COPIAS DE SEGURIDAD, RESPALDO Y RECUPERACIÓN</b>  |  |
| En lo referente a copias de seguridad y protocolo para la realización de las mismas, se debe seguir lo estipulado en el apartado 10.3.6.   |  |
| <b>INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD</b>   |  |
| Para posibles incidencias, incidentes y violaciones relativas a protección de datos, se debe tener presente lo establecido en el apartado 10.3.8 del protocolo.  |  |

## 5. SEGURIDAD DE LA INFORMACIÓN EN LA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES.

|   |   |                        |
|---|---|------------------------|
| <b>Verificación de la existencia de una evaluación de impacto (ámbito de la seguridad).</b> |   |                        |
| <b>¿Existe o se realiza una evaluación de impacto en la organización?</b>                   | SÍ  | NO: No es preciso<br>X |
| <b>Fecha de realización (en su caso):</b>   |   |                        |
| <b>Contenido mínimo de la EIPD según el art. 35.7 del RGPD.</b>                             | Se tendrá presente la información dada a través del presente apartado del protocolo, así como la contenida en los restantes apartados del mismo protocolo.<br>Operaciones de tratamiento: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, |                        |

|  |  |
|--|--|
|  | comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales.  |
| <b>Necesidad y proporcionalidad de las operaciones de tratamiento en relación con los fines:</b>   | Cumplimiento de los principios en favor de la prestación del servicio o finalidad causante.  |
| <p><b>Exigencia de evaluación de impacto motivada por:</b></p> <p>(Debe razonarse el motivo por el que se entiende exigible, teniendo en consideración los criterios y supuestos determinados en el artículo 35 del RGPD así como otros textos complementarios).</p> | <ul style="list-style-type: none"> <li>- Supuestos específicos según el art. 35.1 y .3 del RGPD.</li> <li>- Se utilizan tratamientos con alto riesgo para los derechos y libertades de las personas físicas por su naturaleza, alcance, contexto o fines.</li> <li>- Se realizan tratamientos con grandes volúmenes de datos personales a través de tecnologías como la de los datos masivos (<i>Big data</i>), e internet de las cosas (<i>Internet of Things</i>).</li> <li>- Se utilizan datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.</li> <li>- Se utilizan nuevas tecnologías y tecnologías de videovigilancia a gran escala, aeronaves no tripuladas (drones), vigilancia electrónica, minería de datos (<i>data mining</i>), identificación biométrica, técnicas genéticas, geolocalización sistemática y exhaustiva, o la utilización de etiquetas de radiofrecuencia o RFID.</li> <li>- Entendimiento de exigencia según la siguiente documentación:             <ul style="list-style-type: none"> <li>· Documentos del Comité Europeo de Protección de Datos sobre EIPD.</li> <li>· Directrices sobre la evaluación de impacto relativa a la protección de datos (Criterios para saber si el tratamiento “entraña un alto riesgo”).</li> <li>· <i>Data protection impact assessment template for smart grid and smart metering systems</i>.</li> <li>· Listas de tipos de tratamientos de datos que requieren o no evaluación de impacto relativa a protección de datos, publicadas por la AEPD.</li> </ul> </li> </ul> <p>Todos estos supuestos, condicionados por lo estipulado en el mencionado artículo operante.</p> |
| <b>Riesgos detectados o posibles:</b>  | <ol style="list-style-type: none"> <li>1. Inexistencia de Delegado de Protección de Datos (DPD) cuando sea necesaria su designación.</li> <li>2. Riesgo de no formalizar los contratos con los encargados del tratamiento conforme a la legalidad vigente.</li> <li>3. Deficiencias organizativas en la gestión del control de accesos.</li> <li>4. Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.</li> <li>5. Imposibilidad de identificar usuarios que lleven a cabo acciones en un sistema de información.</li> </ol>   |

|   |  |
|---|--|
|   | <ol style="list-style-type: none"> <li>6. Uso de identificadores que revelan información del afectado.</li> <li>7. Deficiencias en la protección de la confidencialidad de la información.</li> <li>8. Falta de información del personal sobre las medidas de seguridad que están obligadas a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.</li> <li>9. Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.</li> </ol>  |
| <p><b>Medidas adoptadas para afrontar, neutralizar o minimizar los riesgos detectados o posibles:</b></p> | <ol style="list-style-type: none"> <li>1. Designación de DPD cuando proceda.</li> <li>2. Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.</li> <li>3. Políticas estrictas de <i>need to know</i> (necesidad de conocer o acceder a la información) para la concesión de accesos a la información y de <i>clean desks</i> (escritorios limpios) para minimizar las posibilidades de acceso no autorizado a los datos personales.</li> <li>4. Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc.).</li> <li>5. Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones.</li> <li>6. Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y cumplimiento de los compromisos u obligaciones legales de la organización en el área de la protección de datos personales.</li> <li>7. Instalación de herramientas de detección de intrusiones (<i>Intrusion Prevention Systems</i>), complementado con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.</li> <li>8. Implantación de sistemas de <i>Data Loss Prevention</i> o Prevención de Pérdida de Datos, complementado con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.</li> <li>9. Establecer mecanismos de registro de acciones sobre los datos personales o <i>logging</i>, así como herramientas fiables y flexibles de explotación de los ficheros.</li> <li>10. Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales; tales como fecha de nacimiento, nombre y apellidos, etc.</li> </ol> |

|  |  |
|--|--|
|  | <p>11. Adoptar medidas de cifrado adecuadas al riesgo y al estado de la tecnología de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados accedan a ellos ante un hipotético fallo de seguridad.</p> <p>12. Establecer procedimientos de notificación a las personas afectadas para el caso en que sus datos hayan podido ser accedidos o sustraídos por terceros no autorizados, informándoles de las medidas que pueden utilizar para minimizar los riesgos.</p> <p>13. Formación sobre la política de privacidad y seguridad de la organización y, en particular, sobre las obligaciones de cada empleado.</p> |
|--|--|

| <b>GESTIÓN DE RIESGOS</b> |  |   |  |                           |  |   |
|---------------------------|--|---|--|---------------------------|--|---|
| <b>Nº</b>                 | <b>Descripción del riesgo/ amenaza</b> | <b>Nivel de impacto si el riesgo se materializa</b> | <b>Probabilidad de materialización</b> | <b>Medidas propuestas</b> | <b>Nivel de impacto tras la implantación de medidas propuestas</b> | <b>Probabilidad de materialización después de la implantación de las medidas propuestas</b> |
| 1                         |  |   |  |                           |  |   |
| 2                         |  |   |  |                           |  |   |
| 3                         |  |   |  |                           |  |   |
| 4                         |  |   |  |                           |  |   |
| 5                         |  |   |  |                           |  |   |
| ...                       |  |   |  |                           |  |   |

Para la determinación de los valores y el cálculo del riesgo inherente (previo a la determinación de medidas correctoras) y residual (resultado de la implementación de las medidas propuestas), téngase presente las siguientes tablas:

| <b>PROBABILIDAD</b>  |   |
|----------------------|---|
| <b>Despreciable</b>  | La posibilidad de ocurrencia es muy baja    |
| <b>Limitada</b>      | La posibilidad de ocurrencia es baja        |
| <b>Significativa</b> | La posibilidad de ocurrencia es alta        |
| <b>Máxima</b>        | La posibilidad de ocurrencia es muy elevada |

| <b>IMPACTO</b>       |                        |
|----------------------|------------------------|
| <b>Despreciable</b>  | El impacto es muy bajo |
| <b>Limitado</b>      | El impacto es bajo     |
| <b>Significativo</b> | El impacto es alto     |
| <b>Máximo</b>        | El impacto es muy alto |

| CÁLCULO<br>(PROBABILIDAD x IMPACTO) |                 | IMPACTO        |            |                 |          |
|-------------------------------------|-----------------|----------------|------------|-----------------|----------|
|                                     |                 | Despreciable 1 | Limitada 2 | Significativa 3 | Máxima 4 |
| PROBABILIDAD                        | Despreciable 1  | 1              | 2          | 3               | 4        |
|                                     | Limitada 2      | 2              | 4          | 6               | 8        |
|                                     | Significativa 3 | 3              | 6          | 9               | 12       |
|                                     | Máxima 4        | 4              | 8          | 12              | 16       |

| NIVEL DE RIESGO = PROBABILIDAD x IMPACTO |   |
|--|---|
| <b>Bajo</b>                              | Si el valor resultante se sitúa entre los valores 1 y 2     |
| <b>Medio</b>                             | Si el valor resultante es mayor de 2 y menor o igual que 6  |
| <b>Alto</b>                              | Si el valor resultante es mayor que 6 y menor o igual que 9 |
| <b>Muy alto</b>                          | Si el valor resultante es mayor que 9                       |

| RESULTADO DE LA EVALUACIÓN |                  |                 |
|----------------------------|------------------|-----------------|
| Riesgo / Amenaza Nº        | Riesgo inherente | Riesgo residual |
| 1                          |                  |                 |
| 2                          |                  |                 |
| 3                          |                  |                 |
| 4                          |                  |                 |
| 5                          |                  |                 |
| ...                        |                  |                 |

Ello con el fin de comprobar la posible existencia de “alto riesgo” en lo que atañe a los tratamientos y determinar si es preciso o no formalizar consulta previa a la autoridad de control antes de proceder al tratamiento específico; de conformidad con lo regulado en el art. 36 del RGPD.

CONCLUSIÓN: \_\_\_\_\_

## 6. CÓDIGOS DE CONDUCTA EN MATERIA DE PROTECCIÓN DE DATOS.

|   |    |
|---|----|
| Existencia/aplicación de un código de conducta (SÍ/NO): | NO |
| Nombre del código de conducta:                          |    |
| Expedido por:   |    |
| Fecha de aprobación según el art. 40 RGPD:              |    |

## 7. MECANISMOS DE CERTIFICACIÓN EN MATERIA DE PROTECCIÓN DE DATOS.

|  |    |
|--|----|
| Existencia de un mecanismo de certificación (SÍ/NO): | NO |
| Nombre de la certificación:                          |    |
| Expedido por:  |    |
| Periodo de validez (máx. 3 años):                    |    |
| Fecha de aprobación según el art. 42 RGPD:           |    |

## 8. ACTIVOS Y APLICACIONES INFORMÁTICAS.

| ORDENADORES   |     |                                    |                  |   |                   |                        |
|---|-----|------------------------------------|------------------|---|-------------------|------------------------|
|   | SÍ  | NO                                 | Nº DE TERMINALES |   | SISTEMA OPERATIVO | VERSIÓN (SI SE CONOCE) |
| <b>SOBREMESA</b>  | X   |                                    | 5                |   | Windows           |                        |
| <b>PORTATIL</b>   |     | X                                  |                  |   |                   |                        |
| <b>TABLET</b>   |     | X                                  |                  |   |                   |                        |
| <b>OTROS</b>  | TPV |                                    |                  |   |                   |                        |
| INTERNET  |     |                                    |                  |   |                   |                        |
|   | SÍ  | NO                                 | CONTRASEÑA       |   |                   | OTRAS MEDIDAS DE SEG.  |
| <b>WIFI</b>   | X   |                                    | SI               | X | NO                |                        |
| <b>CABLE</b>  |     | X                                  | SI               |   | NO                |                        |
| PROGRAMAS DE GESTIÓN DE DATOS O CON ACCESO A LOS MISMOS |     |                                    |                  |   |                   |                        |
| NOMBRE  |     | EMPRESA COMERCIALIZADORA O GESTORA |                  |   |                   | N.I.F.                 |
| POWER SHOP  |     | POWER SOLUTIONS, S.L.              |                  |   |                   | B80928401              |
|   |     |                                    |                  |   |                   |                        |
|   |     |                                    |                  |   |                   |                        |

## 9. ANÁLISIS DE RIESGOS.

### 9.1 ANÁLISIS BÁSICO DE PROTECCIÓN DE DATOS.

El análisis de riesgos para determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados, se puede compendiar o sintetizar en un enfoque de mínimos, considerando la situación y demás circunstancias específicas a las que se exponen los tratamientos causantes. Ello teniendo presente los criterios actuantes, establecidos en el art. 32 del RGPD. Así pues, se determina el siguiente análisis:

#### 9.1.1 CUADRO DE ANÁLISIS DE RIESGOS.

| TIPOLOGÍA DE DATOS   | SÍ/NO |
|--|-------|
| <b>¿Se van a tratar (1) datos personales (2)? (SÍ/NO)</b>  | SÍ    |
| <i>(1) «Tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.</i>   |       |
| <i>(2) «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.</i> |       |
| Continuar sólo en caso de contestar afirmativamente a la pregunta anterior:  |       |

| FINALIDADES DEL TRATAMIENTO  | DETALLE  | SÍ/NO |
|--|--|-------|
| <i>Marque SÍ/NO (donde aplique) en función de si el tratamiento responde a las siguientes posibles finalidades.</i>  |  |       |
| <b>¿La recogida de los datos tiene como finalidad el tratamiento a gran escala (3)? Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:</b>  |  | NO    |
| <b>El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento):</b>  | <input checked="" type="checkbox"/> de 0 a 10.000<br><input type="checkbox"/> de 10.000 a 100.000<br><input type="checkbox"/> + de 100.000   |       |
| <i>Las categorías de datos tratados. (1. Datos especialmente protegidos, 2. Datos de carácter identificativo, 3. Características personales, 4. Circunstancias sociales, 5. Datos académicos y profesionales, 6. detalles del empleo, 7. Información comercial, 8. Datos económicos, financieros y de seguro, 9. Transacciones de bienes y servicios). Indicar cuántas de estas categorías aplicarían.</i>   | <input type="checkbox"/> 1<br><input checked="" type="checkbox"/> 2<br><input type="checkbox"/> 3<br><input type="checkbox"/> 4<br><input checked="" type="checkbox"/> 5<br><input checked="" type="checkbox"/> 6<br><input checked="" type="checkbox"/> 7<br><input checked="" type="checkbox"/> 8<br><input checked="" type="checkbox"/> 9 |       |
| <b>La duración del tratamiento: instantáneo (I), días (D), semanas (S), meses (M),...</b>  | <input type="checkbox"/> instantáneo <input type="checkbox"/> días<br><input type="checkbox"/> semanas <input checked="" type="checkbox"/> meses   |       |
| <b>La extensión geográfica del tratamiento: Tratamiento a nivel regional (R), nacional (N) o internacional (I):</b>  | <input type="checkbox"/> regional <input checked="" type="checkbox"/> nacional<br><input type="checkbox"/> internacional   |       |
| <b>¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables):</b>   |  | NO    |
| <i>Por ejemplo, uso de registro de actividad sobre clientes para detectar patrones de usuarios susceptibles de contratar un producto, perfiles comerciales, scoring, etc.</i>  |  |       |
| <b>¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos (4)?</b>  |  | NO    |
| <i>(4) Datos identificativos de personas identificadas o identificables asociadas a:</i><br><input type="checkbox"/> Ideología u opiniones políticas.<br><input type="checkbox"/> Afiliación sindical.<br><input type="checkbox"/> Religión u opiniones religiosas.<br><input type="checkbox"/> Creencias o creencias filosóficas.<br><input type="checkbox"/> Origen étnico o racial.<br><input type="checkbox"/> Datos relativos a salud.<br><input type="checkbox"/> Vida sexual u orientación sexual.<br><input type="checkbox"/> Datos de violencia de género y malos tratos.<br><input type="checkbox"/> Datos biométricos dirigidos a identificar de manera unívoca a una persona física (identificación biométrica).<br><input type="checkbox"/> Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica.<br><input type="checkbox"/> Datos solicitados para fines policiales sin consentimiento de las personas afectadas.<br><input type="checkbox"/> Datos relativos a condenas y delitos penales. |  |       |
| <b>¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo (5) o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad (6)?</b>  |  | NO    |
| <i>(5) A modo de ejemplo, las llamadas telefónicas podrían considerarse intrusivas.</i>  |  |       |

|   |    |
|---|----|
| <i>(6) A modo de ejemplo, la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, Big Data o la utilización de etiquetas de radiofrecuencia o RFID10 (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.</i>           |    |
| <b>¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (por ej.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, ...)?</b>   | NO |
| <b>¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones (7)?</b>   | NO |
| <i>(7) A modo de ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales.</i>  |    |
| <b>¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados (8)?</b>   | NO |
| <i>(8) A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones.</i>  |    |
| <b>¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban; en particular, si estas finalidades son más intrusivas o inesperadas para los afectados (9), o incluso pueda llegar a bloquear el disfrute de algún servicio?</b> | NO |
| <i>(9) A modo de ejemplo, el uso de la información contenida en ficheros externos como ASNEF o CIRBE.</i>   |    |
| <b>¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados? Por ejemplo, un departamento que no participe en el tratamiento.</b>  | NO |
| <b>¿Se van a tratar datos relativos a la observación de zonas de acceso público? (por favor, tenga en cuenta que las zonas de acceso público únicamente estarán situadas en la vía pública, excluyendo los lugares de trabajo (por ej.: oficinas comerciales).</b>  | NO |
| <b>Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado (10)?</b>  | NO |
| <i>(10) A modo de ejemplo, utilizar el resultado de un tratamiento de análisis de datos de un cliente para realizarle ofertas comerciales en base a dichos resultados.</i>  |    |
| <b>¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.?</b>   | NO |

| <b>TECNOLOGÍAS EMPLEADAS PARA EL TRATAMIENTO</b>   | <b>SÍ/NO</b> |
|--|--------------|
| <i>Marque SÍ/NO en función de si dichas tecnologías se usan para soportar las finalidades del tratamiento:</i>   |              |
| <b>¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado (11)?</b>   | NO           |
| <i>(11) A modo de ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura.</i> |              |

| CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES DE DATOS  | DETALLE  | SÍ/NO |
|--|--|-------|
| <i>Marque SÍ/NO:</i>   |  |       |
| ¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? En caso afirmativo detallar cuáles.   | Los datos podrán ser cedidos a organismos públicos siempre que procedan las transferencias y/o a entidades privadas por ejecución contractual. | Sí    |
| ¿Se realizan transferencias internacionales de datos a países fuera del Espacio Económico Europeo y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control (12)? (en caso afirmativo detallar cuáles)   |  | NO    |
| <p>(12) A modo de referencia, el siguiente listado contiene los países considerados seguros para las transferencias de datos:</p> <p>__ Andorra.<br/>           __ Argentina.<br/>           __ Canadá (Sector privado).<br/>           __ Suiza.<br/>           __ Islas Feroe.<br/>           __ Guernsey.<br/>           __ Israel.<br/>           __ Isla de Man.<br/>           __ Jersey.<br/>           __ Nueva Zelanda.<br/>           __ Uruguay.<br/>           __ Otros.</p> |  |       |

| PERCEPCIÓN DE LA EXISTENCIA DE RIESGO ELEVADO POR PARTE DEL RESPONSABLE DE LA ACTIVIDAD DE TRATAMIENTO  | DETALLE  | SÍ/NO |
|---|--|-------|
| <i>Marque SÍ/NO:</i>  |  |       |
| ¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD (13)?  |  | NO    |
| <i>(13) En caso afirmativo, se pueden utilizar las conclusiones del EIPD ya realizado para dicho tratamiento.</i>   |  |       |
| ¿Este tratamiento puede conllevar una pérdida o alteración de la información?   |  | NO    |
| ¿Se utilizada documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas: Si, se prevé tratamiento de datos no automatizado |  |       |
| Se guarda bajo llave:   | Archivadores físicos, el acceso restringido a los usuarios indicados en el documento | Sí    |
| Se destruye de forma confidencial:  | Destrucción mediante destructora de papel  | Sí    |
| Se guarda con un registro de accesos:<br>Otros:   |  | NO    |

| TERCEROS QUE INTERVENGAN EN EL TRATAMIENTO   | DETALLE  | SÍ/NO |
|--|--|-------|
| ¿Interviene algún proveedor en el proceso? En caso afirmativo, indicar su denominación social: | ACADEMIA A MARIÑA, S.L.,<br>ASESORÍA J.C. BARREIRO VÁZQUEZ, S.L.,<br>ARVI SISTEMAS AVANZADOS, S.L.,<br>VALORA PREVENCIÓN, S.L. | Sí    |

#### RESULTADO DEL ANÁLISIS

El análisis de riesgos básicos revela que la información tratada y los diversos procesos o procedimientos a los que es sometida no entrañarían un riesgo alto para los datos. Con todo, se estará a lo dispuesto en el apartado 9.2. Las medidas propuestas en el presente documento se adecuan a los posibles riesgos dados, existiendo diversos procedimientos para solventar las posibles incidencias.

Se contemplan las medidas de seguridad necesarias para las diversas fases por las que pasan los datos de carácter personal (apartado 9.3 y 10 del presente protocolo).

En el momento de recogida se proporciona a los interesados la información necesaria de protección de datos, o se solicita el consentimiento del interesado mediante formulario habilitado a tal efecto.

Una vez que la información pasa a las instalaciones de MÍA Y LÍA, S.L.U., esta se gestionará de conformidad con lo establecido en la documentación técnica. Solo tendrá acceso a la información el personal indicado en la documentación. Dicho personal tendrá las directrices de cómo tratar la información y, en caso de duda, deberá consultar al Responsable de Seguridad.

Los datos de carácter personal serán conservados mientras dure la relación comercial/profesional o la finalidad causante y bajo las previsiones legales existentes sobre plazos de conservación, estando sometidos a las directrices indicadas en el presente documento. Una vez cesada la relación comercial/profesional y, teniendo presente los plazos de mantenimiento documental legalmente exigidos, se suprimirán y destruirán tanto los datos personales obrantes en documentación digital como en formato físico. La destrucción de esta última tipología, se hará mediante destructora de papel o empresa habilitada para tal fin. Por último y, en su caso, se dará cumplimiento al art. 32 de la LOPDGDD (bloqueo de datos).

#### 9.1.2 DESCRIPCIÓN DE FLUJOS DE INFORMACIÓN: CICLO DE VIDA DE LOS DATOS.

| MODELO PARA LA DESCRIPCIÓN DE FLUJOS DE LA INFORMACIÓN |   |  |   |  |  |   |
|--|---|--|---|--|--|---|
| Nº   | Descripción   | Origen de la información                               | Destinatarios de la info.   | Categorías de Datos  | Finalidad  | Causas legitimadoras  |
| 1  | Información relativas a 'CLIENTES, USUARIOS Y OTROS INTERESADOS'. | La información es facilitada por el propio interesado. | Organismos públicos para cumplimiento de obligaciones legales. Bancos y cajas de ahorros. | Nombre y apellidos, DNI, domicilio, teléfono, mail, datos bancarios. | Información necesaria para la correcta gestión de la relación comercial. | Relación contractual, consentimiento otorgado o interés legítimo del responsable, según caso. |

|   |  |   |   |  |   |  |
|---|--|---|---|--|---|--|
| 2 | Información relativa a 'PROVEEDORES'.                                    | La información es facilitada por el propio interesado.  | Organismos públicos para cumplimiento de obligaciones legales. Bancos y cajas de ahorros. | Razón social, NIF, domicilio, teléfono, mail, datos bancarios, datos de transacciones comerciales. | Correcto mantenimiento de la relación comercial entre partes.   | Relación contractual o interés legítimo del responsable. |
| 3 | Información relativa a 'NÓMINAS Y RR.HH'                                 | La información es facilitada por el propio interesado.  | Organismos públicos para cumplimiento de obligaciones legales. Bancos y cajas de ahorros. | Nombre y apellidos, domicilio, teléfono, mail, datos académicos, detalles de puestos de trabajo.   | Correcto mantenimiento de la relación laboral mantenida y participación en procesos de selección de personal. | Relación contractual laboral o consentimiento otorgado.  |
| 4 | Información relativa a 'ACCESO A LAS INSTALACIONES Y REGISTRO'           | La información es recabada por el Responsable directamente.   | No se prevé cesiones de información.  | Información del afectado que accede a las instalaciones.   | Seguridad de las instalaciones.   | Interés legítimo del responsable.                        |
| 5 | Información relativa a 'USUARIOS WEB Y OTRAS PLATAFORMAS Y APLICACIONES' | La información es recabada por el Responsable en determinados supuestos o facilitada por el propio interesado en otros. | No se prevé cesiones de información.  | Dir. IP, datos de contacto, nombre, apellidos, domicilio, mail y teléfono.                         | Atención a las consultas planteadas por el usuario/cliente.   | Consentimiento del usuario/cliente.                      |

Nota: para completar y complementar la presente tabla, véase el registro de actividades de tratamiento y los ficheros descritos en el presente protocolo.

En cuanto a tecnologías intervinientes y destrucción de los datos, se estará a lo dispuesto en el precedente apartado relativo al cuadro de análisis y su resultado (además del apartado octavo sobre activos y aplicaciones informáticas).

| <b>Modelo relativo a roles</b> |  |
|--------------------------------|--|
| Interesados                    |  |
| Responsable del tratamiento    |  |
| Encargados de tratamiento      |  |
| Terceras partes involucradas   |  |

| <b>Modelo relativo a descripción sistemática de las operaciones y finalidades del tratamiento</b>                          |  |
|--|--|
| Principales transferencias / envíos de datos.  |  |
| Flujos de datos entre sistemas.  |  |
| Productos o servicios generados por procesamiento de los datos.  |  |
| Procedimiento para cumplir el deber de información, en caso de que se recojan los datos directamente del interesado.       |  |
| Procedimiento para la solicitud de consentimiento, en caso de que se recojan los datos directamente del interesado.        |  |
| Procedimiento para el ejercicio de los derechos por parte de los interesados.  |  |
| Se considera la identificación de las obligaciones y medidas de seguridad de los encargados de tratamiento en su contrato. |  |
| En caso de existir transferencias internacionales fuera del Espacio Económico Europeo, estas son adecuadamente protegidas. |  |

## 9.2 IDENTIFICACIÓN DE LOS RIESGOS.

Los riesgos pueden ser de dos tipos:

- El primero y principal, es el que afecta a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.
- El segundo obedece a la materia de riesgos que puede afrontar una organización por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descuidada o errónea, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces.

A continuación, teniendo en cuenta los activos existentes y su posible afectación, se detallan, como alcance, una serie de riesgos cuya presencia deberá ser comprobada y, en caso de detectarlos sin poder ser evitados, teniendo presente la determinación y valoración cualitativa del propio riesgo, se deberán adoptar las medidas necesarias para eliminarlos o, si ello no es posible, al menos mitigarlos, transferirlos o asumirlos del mejor modo posible.

A mayores y, a razón de tales posibles riesgos, se prestará la debida atención al listado de cumplimiento normativo publicado por la AEPD, en favor de la disposición de un *método básico que permita identificar los requisitos de cumplimiento del Reglamento General de Protección de Datos (RGPD) con el objeto de poder valorar los aspectos que deben tener en cuenta durante los procesos de análisis de riesgos y evaluación de impacto* <https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf>

| <b>RIESGOS/AMENAZAS</b>   |
|---|
| <b>Generales:</b>   |
| <ul style="list-style-type: none"> <li>• Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos.</li> <li>• Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el Responsable del tratamiento.</li> </ul> |

|  |
|--|
| <ul style="list-style-type: none"> <li>• Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas; en particular, cuando se producen pérdidas de datos personales.</li> <li>• Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad.</li> <li>• Falta de conocimiento experto o incorporación tardía sobre protección de datos (en particular, del Delegado de Protección de Datos o DPD) o definición deficiente de sus funciones y competencias.</li> <li>• Daños físicos (fuego, agua, desastres naturales, etc.).</li> <li>• Corte de suministro eléctrico, condiciones inadecuadas, fallo de servicios de comunicaciones, interrupción de otros servicios y suministros y desastres industriales.</li> <li>• Denegación del servicio, robo, extorsión, ingeniería social.</li> </ul>   |
| <p><b>Legitimación de los tratamientos y cesiones de datos personales:</b></p> <ul style="list-style-type: none"> <li>• Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida.</li> <li>• Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.</li> <li>• Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.</li> <li>• Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.</li> <li>• Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.</li> <li>• Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.</li> <li>• Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros; en particular, la re-identificación de información disociada.</li> <li>• Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada.</li> <li>• Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.</li> </ul> |
| <p><b>Transferencias internacionales:</b></p> <ul style="list-style-type: none"> <li>• Acceso secreto a los datos personales por parte de autoridades de terceros países u organizaciones internacionales.</li> <li>• Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.</li> <li>• Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados.</li> <li>• Incapacidad de ayuda a los ciudadanos en el ejercicio de sus derechos ante el importador.</li> <li>• No obtención de las autorizaciones legales necesarias.</li> </ul>   |
| <p><b>Transparencia de los tratamientos:</b></p> <ul style="list-style-type: none"> <li>• Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.).</li> <li>• En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que dificulten su acceso conjunto y detallado.</li> </ul>  |

|  |
|--|
| <ul style="list-style-type: none"> <li>• Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.</li> </ul>   |
| <p><b>Calidad de los datos:</b></p> <ul style="list-style-type: none"> <li>• Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio.</li> <li>• Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias; lo que puede derivar en la toma de decisiones erróneas.</li> <li>• Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.</li> <li>• Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas; datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas; toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables) especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes del servicios y productos o trabas para el paso de fronteras; toma de decisiones automatizadas con posibles consecuencias relevantes para las personas; utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.</li> <li>• Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo.</li> <li>• Carecer de procedimientos claros y de herramientas adecuadas para garantizar la supresión de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades que se recogieron.</li> <li>• Fuga de información; información falsa. Alteración, corrupción, destrucción e interceptación de información.</li> <li>• Degradación de soportes; software dañino; errores de mantenimiento y actualización de programas y equipos; caída del sistema; pérdida de equipos, terminales y dispositivos.</li> <li>• Errores de usuarios, administradores y configuración.</li> </ul> |
| <p><b>Datos especialmente protegidos:</b></p> <ul style="list-style-type: none"> <li>• Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión.</li> <li>• Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles.</li> <li>• Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo contemplen utilizar datos anónimos.</li> </ul>   |
| <p><b>Deber de secreto:</b></p> <ul style="list-style-type: none"> <li>• Accesos no autorizados a datos personales.</li> <li>• Violaciones de la confidencialidad de los datos personales por parte de los empleados u otros agentes de la organización.</li> <li>• Indisponibilidad del personal, abuso de privilegios de acceso y accesos no autorizados.</li> </ul>   |

| <b>Encargado del tratamiento:</b>  |
|--|
| <ul style="list-style-type: none"> <li>• Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.</li> <li>• Falta de diligencia (o dificultad para demostrarla) en la elección del encargado del tratamiento.</li> <li>• Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.</li> <li>• No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos del interesado (acceso, rectificación, supresión...) realizados ante los encargados de tratamiento.</li> <li>• Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.</li> </ul>   |
| <b>Derechos del afectado:</b>  |
| <ul style="list-style-type: none"> <li>• Dificultar o imposibilitar el ejercicio de los derechos del afectado (información, acceso, rectificación, supresión...)</li> <li>• Carencia de procedimientos y herramientas para la gestión de los derechos.</li> <li>• Carencia de procedimientos y herramientas para la comunicación de rectificaciones, supresiones u oposiciones a los cesionarios de los datos personales.</li> </ul>   |
| <b>Seguridad de la información:</b>  |
| <ul style="list-style-type: none"> <li>• Inexistencia de Responsable de Seguridad o deficiente definición de sus funciones y competencias.</li> <li>• Inexistencia de Delegado de Protección de Datos cuando es preciso su designación.</li> <li>• Inexistencia de política de seguridad.</li> <li>• Deficiencias organizativas en la gestión de control de accesos.</li> <li>• Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.</li> <li>• Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.</li> <li>• Uso de identificadores que revelan información del afectado.</li> <li>• Deficiencias en la protección de la confidencialidad de la información.</li> <li>• Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.</li> <li>• Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc...) para terceros no autorizados.</li> </ul> |

A la hora de calcular el riesgo, optando por un análisis cualitativo y teniendo presente posibles vulnerabilidades y salvaguardas, se hará uso de una matriz de riesgo, como la representada a continuación y con las siguientes tablas de cálculo:

| <b>TABLA PARA ESTIMAR LA PROBABILIDAD</b> |  |
|---|--|
| <b>Valor</b>                              | <b>Descripción</b>                                       |
| Bajo                                      | La amenaza se materializa a lo sumo una vez cada año.    |
| Medio                                     | La amenaza se materializa a lo sumo una vez cada mes.    |
| Alto                                      | La amenaza se materializa a lo sumo una vez cada semana. |

| TABLA PARA ESTIMAR EL IMPACTO |  |
|-------------------------------|--|
| Valor                         | Descripción  |
| Bajo                          | El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.     |
| Medio                         | El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.        |
| Alto                          | El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización. |

| CÁLCULO DEL RIESGO |       | Impacto  |       |          |
|--------------------|-------|----------|-------|----------|
|                    |       | Bajo     | Medio | Alto     |
| Probabilidad       | Bajo  | Muy bajo | Bajo  | Medio    |
|                    | Medio | Bajo     | Medio | Alto     |
|                    | Alto  | Medio    | Alto  | Muy alto |

### 9.3 GESTIÓN DE LOS RIESGOS IDENTIFICADOS.

Una vez que se han identificado los riesgos con valor superior a “medio” a través del análisis llevado a cabo y, tras atender a los resultados de las consultas internas y externas, llega el momento de gestionar dichos riesgos.

En la teoría general del análisis de riesgos, se contemplan diversas opciones de gestión, dependiendo del impacto que su materialización tendría para la organización: evitarlo, eliminarlo, mitigarlo, transferirlo o asumirlo.

A continuación, se incluyen algunas medidas correctoras que se podrían adoptar para gestionar tales riesgos, identificados por tipologías, que pueden haberse detectado en la fase anterior. Ello teniendo por posible la vinculación de determinados derechos y libertades de los interesados; tales como los contemplados en los arts. 16, 18, 20, 22, 23, 24, 27 y 28 de la Constitución Española u otros:

| GENERALES:  |  |
|---|--|
| RIESGOS/AMENAZAS  | MEDIDAS/SOLUCIONES   |
| Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.   | -Formación apropiada del personal sobre protección de datos.<br>-Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización, así como de las sanciones aparejadas al incumplimiento de las mismas.   |
| Pérdidas económicas, pérdidas de clientes y daños reputacionales derivados del incumplimiento de legislaciones sectoriales o por carencia de medidas de seguridad o ineficacia de estas, con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento. | -Formación apropiada del personal sobre protección de datos en el sector específico que se trate.<br>-Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas de privacidad de la organización, relativas a las legislaciones sectoriales que afectan a la organización; así como de las sanciones aparejadas al incumplimiento de las mismas. |
| Pérdida de competitividad del producto o servicio derivada de los   | -Formación apropiada del personal sobre protección de datos, seguridad y uso adecuado de las TIC.  |

|   |  |
|---|--|
| daños reputacionales causados por una deficiente gestión de la privacidad de las personas.  |  |
| Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.   | -Nombrar a una persona o departamento como responsable de interlocución con los afectados en todo aquello relativo a la privacidad y la protección de datos personales, y comunicar claramente la forma de contactar con ella.<br>Nombrar un Delegado de Protección de Datos o <i>Data Protector Officer</i> (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado.  |
| Incorporación tardía de los expertos en protección de datos (en particular, del Delegado de Protección de Datos o DPD) al proyecto o definición deficiente de sus funciones y competencias. | -Incluir dentro de los procedimientos de diseño y desarrollo de nuevos productos y servicios la incorporación del DPD en el desarrollo y gestión de los proyectos.   |
| Daños físicos (fuego, agua, desastres naturales, etc.).   | -Establecer protocolos de actuación y simulacros.  |
| Corte de suministro eléctrico, condiciones inadecuadas, fallo de servicios de comunicaciones, interrupción de otros servicios y suministros y desastres industriales.                       | -Establecer protocolos de actuación y simulacros.  |
| Denegación del servicio, robo, extorsión, ingeniería social.  | -Establecer protocolos de actuación y simulacros.  |
| <b>LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE LOS DATOS PERSONALES:</b>   |  |
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>  |
| Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida.  | -Usar datos disociados siempre que sea posible y no implique un esfuerzo desproporcionado.<br>-Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas.<br>-Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.<br>-Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas.<br>-Evitar el uso de datos biométricos salvo que resulte imprescindible o este absolutamente justificado. |
| Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.   | -Formación adecuada del personal sobre protección de datos, seguridad y uso adecuado de las TIC.<br>-Revisar las posibilidades y habilitaciones que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas.   |

|   |  |
|---|--|
|   | <p>-Si es necesario, buscar asesoramiento experto.</p> <p>-Si se ceden datos personales, establecer por escrito acuerdos que contemplen las condiciones bajo las que se produce la cesión y, en su caso, las relativas a cesiones posteriores, así como las posibilidades de supervisión y control del cumplimiento del acuerdo.</p>   |
| <p>Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.</p>               | <p>-Asegurarse de que no existen otras causas de legitimación más adecuadas.</p> <p>-Cuando el tratamiento de datos personales se legitime por una relación contractual, ofrecer siempre la posibilidad de consentimiento separado para tratar datos con finalidades que no son necesarias para el cumplimiento o perfeccionamiento de la misma, evitando incluirlas de forma indisoluble en las cláusulas del contrato.</p> <p>-Evitar condicionar el disfrute de un producto o servicio al consentimiento para finalidades diferentes.</p> <p>-En el ámbito laboral, evitar basar los tratamientos de datos en el consentimiento de los trabajadores.</p> <p>-Evitar forzar el consentimiento desde una posición de prevalencia del responsable o cuando existen otras causas legitimadoras suficientes y más adecuadas.</p> |
| <p>Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.</p>            | <p>-Establecer procedimientos claros para manifestar la revocación del consentimiento o la solicitud de oposición a un determinado tratamiento. Si la organización realiza acciones publicitarias, tener en cuenta las reglas especiales existentes para las comunicaciones comerciales y, en particular, cuando estas se lleven a cabo a través de comunicaciones electrónicas.</p> <p>-Establecer los mecanismos necesarios para garantizar que se consultan los ficheros de exclusión de publicidad, tanto de la organización como externos, y que se tienen en cuenta los deseos de quienes se han inscrito en ellos.</p>  |
| <p>Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.</p> | <p>-Exigir garantías de que los datos personales provenientes de terceros se han obtenido y cedido legal y lealmente.</p> <p>-En la realización de campañas publicitarias con datos provenientes de terceros en las que se segmenta el público objetivo en función de parámetros determinados, exigir garantías de que las personas cuyos datos van a ser utilizados han dado su consentimiento para ello.</p>   |
| <p>Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias.</p>          | <p>-Verificar que el tratamiento de datos especialmente protegidos es absolutamente imprescindible para la finalidad o finalidades perseguidas.</p> <p>-Verificar si el tratamiento está amparado o es requerido por una ley.</p> <p>En caso contrario, establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.</p>  |

|  |  |
|--|--|
| Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada. | <ul style="list-style-type: none"> <li>-Verificar la legitimidad de la interconexión de datos prevista.</li> <li>-Definir claramente los datos personales resultantes del tratamiento y verificar tras el proceso que son los únicos que se han generado.</li> </ul>   |
| Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada   | <ul style="list-style-type: none"> <li>-Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies.)</li> <li>-Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas.</li> <li>-Respetar las preferencias establecidas por los afectados en sus navegadores sobre el rastreo de su navegación.</li> </ul> |
| Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.  | <ul style="list-style-type: none"> <li>-Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas.</li> </ul>   |
| <b>TRANSFERENCIAS INTERNACIONALES DE DATOS:</b>  |  |
| <b>RIESGOS/AMENAZAS</b>  | <b>MEDIDAS/SOLUCIONES</b>  |
| Acceso secreto a los datos personales por parte de autoridades de terceros países u organizaciones internacionales.  | <ul style="list-style-type: none"> <li>-Incluir cláusulas de salvaguarda en las que se requiera información sobre acceso a los datos personales transferidos por parte de autoridades de terceros países tan pronto como sea posible.</li> </ul>   |
| Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.   | <ul style="list-style-type: none"> <li>-Si existen transferencias internacionales a países fuera del Espacio Económico Europeo, implantar los procedimientos de control necesarios (incluidos los contractuales) para garantizar que se cumplen las condiciones bajo las que se llevó a cabo la transferencia. En este sentido, hay que prestar especial atención cuando se contraten servicios de <i>cloud computing</i> u hospedados en terceros.</li> </ul>   |
| Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados.   | <ul style="list-style-type: none"> <li>-Tomar medidas de exigencia y accionamiento de mecanismos de control del importador; tales como listas de encargados del tratamiento, de países donde operan, posibilidad de realizar auditorías y revisar la documentación, etc.</li> </ul>  |
| Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador.   | <ul style="list-style-type: none"> <li>-Asegurarse de la definición y funcionamiento de un canal de comunicación entre exportador e importador para hacer llegar las solicitudes y reclamaciones de los afectados.</li> </ul>  |
| No obtención de las autorizaciones legales necesarias.   | <ul style="list-style-type: none"> <li>-Solicitar la autorización de la Agencia Española de Protección de Datos en aquellos casos que resulte necesario.</li> </ul>  |

| <b>TRANSPARENCIA DE LOS DATOS:</b>  |  |
|---|--|
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>  |
| <p>Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.).</p>  | <p>-Informar con transparencia sobre el uso y finalidades de las cookies. En particular, esta información se podrá ofrecer a través de un sistema de capas.<br/>-Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrece la información adecuada.</p> |
| <p>En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que hagan muy difícil su acceso conjunto y detallado.</p>   | <p>-Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas gráficos para facilitar su comprensión.<br/>-Verificar que la información que se ofrece en todos los lugares y situaciones es coherente y sistemática.<br/>-Verificar que la información que se ofrece en todos los formularios.</p>                    |
| <p>Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.</p> | <p>-Implantar políticas de privacidad, claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.</p>   |
| <b>CALIDAD DE LOS DATOS:</b>  |  |
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>  |
| <p>Solicitar datos o categorías de datos innecesarios para las finalidades del sistema o producto.</p>  | <p>-Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.</p>  |
| <p>Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias; lo que puede derivar en toma de decisiones erróneas.</p>          | <p>-Establecer medidas técnicas y organizativas que garanticen que las actualizaciones de datos de los afectados se comunican a todos los sistemas de información y departamentos de la organización que estén autorizados a utilizarlos.</p>  |
| <p>Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.</p>  | <p>-Siempre que sea posible, utilizar datos anónimos o disociados.<br/>-Utilizar pseudónimos o atribuir códigos de sustitución de los datos identificativos que, aunque no consigan la disociación absoluta de los mismos, sí se pueden contribuir a que la información sobre la identidad de los afectados solo sea accesible a un número reducido de personas.</p>   |

|   |   |
|---|---|
|   | -Garantizar que se aplican las medidas de seguridad, adecuadas y correspondientes al nivel de seguridad de los datos utilizados.  |
| <p>-Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas.</p> <p>-Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas.</p> <p>-Toma de decisiones económicas, sociales, laborales, etc., relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables) especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes del servicios y productos o trabas para el paso de fronteras.</p> <p>-Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.</p> <p>-Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.</p> | <p>-Suministrar información transparente y clara sobre las finalidades para las que se tratarán los datos personales, en particular, a través de una política de privacidad visible y accesible.</p> <p>-Proporcionar información sobre los criterios utilizados en la toma de decisiones y permitir a los afectados impugnar la decisión y solicitar que sea revisada por una persona.</p> <p>-Proporcionar información sobre las medidas que se han implantado para lograr el necesario equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los afectados.</p> |
| Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo.   | <p>-Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer.</p> <p>-Establecer posibilidades de impugnación ágiles para ofrecer vías de recurso adecuadas a los afectados.</p> <p>Establecer canales alternativos para tratar con los falsos negativos y falsos positivos en la identificación y autenticación de personas a través de datos biométricos.</p>   |
| Carecer de procedimientos claros y de herramientas adecuadas para garantizar la supresión de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades que se recogieron.   | <p>-Definir claramente los plazos de supresión de todos los datos personales de los sistemas de información.</p> <p>-Establecer controles automáticos dentro de los sistemas de información para avisar de la cercanía de los plazos de supresión de la información.</p> <p>-Implantar mecanismos para llevar a cabo y gestionar dicha supresión en el momento adecuado incluyendo, si corresponde, el bloqueo temporal de los datos personales.</p>  |
| Fuga de información; información falsa. Alteración, corrupción, destrucción e interceptación de información.  | <p>-Establecimiento de cadena de custodia de dispositivos de almacenamiento externo.</p> <p>-Identificación externa de los dispositivos.</p> <p>-Establecimiento de claves de acceso a la información.</p> <p>-Seudonimización de la información contenida.</p>   |

|  |  |
|--|--|
| Degradación de soportes; software dañado; errores de mantenimiento y actualización de programas y equipos; caída del sistema; pérdida de equipos, terminales y dispositivos. | -Establecer protocolos de actuación y simulacros.<br>-Adquisición y utilización de software que haga frente a tales posibles situaciones y circunstancias.<br>-Adquisición de equipos auxiliares.  |
| Errores de usuarios, administradores y configuración.  | -Establecer protocolos de actuación y simulacros.  |
| <b>DATOS ESPECIALMENTE PROTEGIDOS:</b>   |  |
| <b>RIESGOS/AMENAZAS</b>  | <b>MEDIDAS/SOLUCIONES</b>  |
| Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión.                            | -Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario.<br>-Establecer procedimientos que garanticen la obtención del consentimiento expreso y que permitan probar que se cuenta con él.   |
| Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos sensibles.   | -Nombrar un Delegado de Protección de Datos o <i>Data Protection Officer</i> (DPD) para contar con asesoramiento cualificado.  |
| Disociación deficiente o reversible que permita la re-identificación de datos sensibles en procesos de investigación que solo prevén utilizar datos anónimos.                | -Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación es mínimo.   |
| <b>DEBER DE SECRETO:</b>   |  |
| <b>RIESGOS/AMENAZAS</b>  | <b>MEDIDAS/SOLUCIONES</b>  |
| Accesos no autorizados a datos personales.   | -Establecer mecanismos y procedimientos de concienciación y garantía sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales.<br>-Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización.<br>-Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores/profesionales/funcionarios u otros agentes que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento.<br>-Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales.<br>-Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales. |
| Violaciones de la confidencialidad de los datos personales por parte de los empleados u otros agentes de la organización.  | -Medidas de asunción y formación adecuada de los empleados/profesionales/funcionarios u otros agentes sobre sus obligaciones y responsabilidades respecto a la confidencialidad de la información.<br>-Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas.   |

|   |   |
|---|---|
| Indisponibilidad del personal, abuso de privilegios de acceso y accesos no autorizados.   | -Establecimiento de cadena de custodia de dispositivos de almacenamiento externo.<br>-Identificación externa de los dispositivos.<br>-Establecimiento de claves de acceso a la información.<br>-Seudonimización de la información contenida.  |
| <b>TRATAMIENTOS POR ENCARGO:</b>  |   |
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>   |
| Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.   | Establecer procedimientos que garanticen que siempre que se recurre a un encargado del tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.   |
| Falta de diligencia (o dificultad para demostrarla) en la elección de encargado del tratamiento.  | Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas; a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas y mecanismos de certificación homologados y de acreditada solvencia.<br>-Establecer contractualmente posibles mecanismos de supervisión, verificación y auditoría de los tratamientos encargados a terceros.                                    |
| Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. | -Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que pueda elegir un encargado del tratamiento.<br>-Realizar posibles auditorías periódicas u otras acciones de supervisión al encargado del tratamiento para verificar que cumple las estipulaciones del contrato.<br>-Definir acuerdos de nivel de servicio que garanticen el correcto cumplimiento de las instrucciones del responsable y la adopción de medidas de seguridad adecuadas. |
| No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARSOPL u otros realizados ante los encargados de tratamiento.   | -Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos ARSOPL u otros.<br>-Definir los procedimientos operativos para que esta comunicación se lleve a cabo de forma ágil y eficiente.  |
| Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.  | -Incluir la obligación de portabilidad en el contrato y en los acuerdos de nivel de servicio.<br>-Establecer medidas técnicas y organizativas que garanticen la portabilidad.   |
| <b>DERECHOS DE LOS INTERESADOS:</b>   |   |
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>   |
| Dificultar o imposibilitar el ejercicio de los derechos.  | -Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos ARSOPL u otros.<br>-Evitar sistemas de ejercicio de los derechos ARSOPL u otros que impliquen solicitar una remuneración.   |

|   |  |
|---|--|
|   | <ul style="list-style-type: none"> <li>-Evitar establecer procedimientos poco transparentes, complejos y laboriosos.</li> <li>-Formar a todo el personal para que conozca qué ha de hacer si recibe una petición de derecho ARSOPL u otro o ha de informar a los afectados sobre como ejercerla.</li> <li>-Definir qué personas o departamentos se ocuparán de gestionar los derechos ARSOPL u otros y formarlos adecuadamente.</li> </ul>   |
| Carencia de procedimientos y herramientas para la gestión de derechos ARSOPL u otros.   | <ul style="list-style-type: none"> <li>-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen que todos los empleados conocen cómo actuar ante un ejercicio de derechos ARSOPL u otros y que puedan suministrar la información adecuada a los afectados.</li> <li>-Formación de los empleados encargados de gestionar los ejercicios de derechos ARSOPL u otros.</li> </ul>  |
| Carencia de procedimientos y herramientas para la comunicación de rectificaciones, supresiones u oposiciones a los cesionarios de los datos personales. | <ul style="list-style-type: none"> <li>-Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, supresiones y oposiciones a las organizaciones a las que se hayan cedido los datos personales que se traten.</li> <li>-Establecimiento de acuerdos y procedimientos de gestión y comunicación con los cesionarios de la información que garanticen la correcta actualización de los datos personales cedidos.</li> <li>-Formación de los empleados encargados de gestionar los ejercicios de los derechos ARSOPL u otros.</li> </ul>   |
| <b>SEGURIDAD:</b>   |  |
| <b>RIESGOS/AMENAZAS</b>   | <b>MEDIDAS/SOLUCIONES</b>  |
| Inexistencia de DPD cuando es precisa su designación o del responsable de seguridad o deficiente definición de sus funciones y competencias.            | <ul style="list-style-type: none"> <li>-Nombramiento, en su caso, del DPD y del responsable de seguridad y establecimiento por parte de la dirección, de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos.</li> <li>-Incluir dentro de los procedimientos de diseño y desarrollo y gestión de los proyectos.</li> </ul>  |
| Deficiencias organizativas en la gestión del control de accesos.  | <ul style="list-style-type: none"> <li>-Políticas estrictas de <i>need to know</i> (necesidad de conocer o acceder a la información) para la concesión de accesos a la información y de <i>clean desks</i> (escritorios limpios) para minimizar las posibilidades de acceso no autorizado a los datos personales.</li> <li>-Establecer procedimientos que garanticen la revocación de permisos para acceder a datos personales cuando ya no sean necesarios (abandono de la organización, traslado, cambio de funciones, etc...).</li> <li>-Inventariar los recursos que contengan datos personales accesibles a través de redes de telecomunicaciones.</li> </ul> |
| Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.                          | <ul style="list-style-type: none"> <li>-Instalar herramientas de <i>hardware</i> o <i>software</i> que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de los datos personales.</li> </ul>   |

|  |   |
|--|---|
|  | <p>-En el caso de que pudiera resultar necesario, instalar herramientas de detección de intrusiones y/o prevención de intrusiones con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.</p> <p>-En la medida que pudiera resultar necesario, implantar sistemas de <i>Data Loss Prevention</i> o Prevención de Pérdida de datos con la necesaria información a los trabajadores sobre su instalación, características e implicaciones para su privacidad.</p>   |
| Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.   | -Establecer mecanismos de registro de acciones sobre los datos personales o <i>logging</i> así como herramientas fiables y flexibles de control de explotación de los ficheros.   |
| Uso de identificadores que revelan información del afectado.   | <p>-Establecer políticas de asignación de códigos de usuario por parte de la organización que eviten datos triviales como fecha de nacimiento, nombre y apellidos, etc.</p> <p>-Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o simuladores, ya que favorecen el fraude en la autenticación e incluso la suplantación de identidad.</p>  |
| Deficiencias en la protección de la confidencialidad de la información.  | <p>-Adoptar medidas de cifrado adecuadas al riesgo y al estado de la tecnología de los datos personales almacenados y compartidos a través de redes de telecomunicaciones (en particular, si son públicas y/o inalámbricas) para minimizar el riesgo de que terceros no autorizados acceden a ellos ante un hipotético fallo de seguridad.</p> <p>-Establecer procedimientos de notificación a las personas afectadas para el caso en que sus datos hayan podido ser accedidos o sustraídos por terceros no autorizados, informándoles de las medidas que pueden utilizar para minimizar los riesgos.</p> <p>-Establecer procedimientos de notificación de quiebras de seguridad a la autoridad de control cuando ello no sea legalmente exigible.</p> <p>-Evitar, en general, las pruebas con datos reales y, en particular, cuando incluyan datos especialmente protegidos o un conjunto importante de datos que revelan aspectos relevantes de la personalidad de los afectados, cuando se empleen los de muchas personas o cuando participen en las pruebas un número elevado de usuarios.</p> <p>-Construir canales seguros y con verificación de identidad para la distribución de información.</p> |
| Inexistencia de política de seguridad y de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden | <p>-Implementación y formación sobre la política de seguridad de la organización y, en particular, sobre las obligaciones de cada empleado.</p> <p>-Comunicación auditable y clara de las responsabilidades del personal en relación con el</p>   |

|   |  |
|---|--|
| derivar de no hacerlo.  | cumplimiento de las políticas y las medidas de seguridad, así como de las sanciones aparejadas al incumplimiento de las mismas.  |
| Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados. | <ul style="list-style-type: none"> <li>- Establecer medidas de control de acceso a datos tanto en soporte físico como en digital: Registro de accesos, etc.</li> <li>- Establecimiento de medidas formativas.</li> </ul> |

## **10. MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS ADECUADAS AL RIESGO PARA LOS DATOS OBJETO DE TRATAMIENTO EN LA ORGANIZACIÓN.**

Se trata de un conjunto de medidas enfocadas a garantizar un nivel de seguridad adecuado al riesgo en la entidad, según lo dispuesto por el artículo 32 del RGPD.

Con todo, se entenderán también como actuantes las directrices dadas por la *Guía de protección de datos por defecto*, elaborada por la AEPD en octubre de 2020. En especial, se ejecutarán las siguientes previsiones:

- Determinar los datos mínimos necesarios para cada tratamiento, independientemente de los que se encuentren disponibles.
- Realizar una separación lógica y/o física de datos personales utilizados en cada tratamiento.
- Gestionar los derechos de acceso de acuerdo con cada tratamiento.
- Establecer un espacio independiente, que podría ser lógico o físico, dependiendo de los casos, para los tratamientos de datos sensibles (*en su caso*).

Ya teniendo presente el mencionado art. 32 del Reglamento 2016/679 y sus criterios operantes, se determinan las siguientes medidas:

### **10.1 SEUDONIMIZACIÓN.**

La seudonimización es el tratamiento de datos personales de tal manera que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. Es decir, la seudonimización reduce la vinculación de un conjunto de datos con la identidad original del interesado.

| <b>MEDIDAS CONTEMPLADAS PARA LA SEUDONIMIZACIÓN DE DATOS PERSONALES<br/>(de ser procedente)</b> |                      |
|---|----------------------|
| <b>Técnicas</b>   | <b>Organizativas</b> |
| Uso de listas de correspondencia.   |                      |
| Empleo de algoritmos criptográficos bidireccionales.  |                      |
| Encriptado, funciones hash, tokenización, etc.  |                      |
| Otros:  |                      |

## 10.2 CIFRADO DE DATOS PERSONALES.

| MECANISMOS DE CIFRADO A UTILIZAR POR LA ORGANIZACIÓN (de ser procedente)  |                             |
|---|-----------------------------|
| Mecanismo   | Ficheros de datos afectados |
| Cifrado convencional y alternativas al cifrado convencional ( <i>esteganografía y Spread-spectrum</i> ).  |                             |
| Criptografía de clave privada o simétrica: DES, Triple DES, DESX: aplicaciones bancarias, EFS, DEA: PGP, RC4, RC5: SSL; AES: Rijndael, Blowfish, Twofish, CAST, SAFER, etc.   |                             |
| Criptografía de clave pública o asimétrica: RSA, Diffie-Hellman, El Gamal, Algoritmos de curva elíptica, etc.   |                             |
| Empleo de funciones resumen o hash: MD4, MD5, SHA, SHA 1, SHA 256, RIPEMD160, etc.  |                             |
| Infraestructuras de Clave Pública (ICPs o PKIs, <i>Public Key Infrastructures</i> , etc.).  |                             |
| FPE, cifrado analógico de voz, cifrado autenticado, cifrado autosíncrono, cifrado de archivos, cifrado de columnas en bases de datos, cifrado de disco, cifrado de flujo, cifrado del enlace, cifrado de texto con voz auto-clave, cifrado en bloque, cifrado extremo a extremo, cifrado reversible, cifrado irreversible, cifrado masivo, cifrado Vernam, etc. |                             |
| Otros:  |                             |

## 10.3 MEDIDAS DE SEGURIDAD QUE GARANTIZAN LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA PERMANENTES DE LOS SISTEMAS Y SERVICIOS DE TRATAMIENTO EN LA ENTIDAD.

### 10.3.1 IDENTIFICACIÓN Y AUTENTICACIÓN. USUARIOS AUTORIZADOS.

El acceso físico a la documentación solo se podrá llevar a cabo por el personal expresamente autorizado. Este personal tendrá llave que le permita el acceso a los archivadores donde se encuentra la documentación. En caso de que personal no autorizado tenga acceso a la información deberá dejar constancia en hoja de registro habilitada a tal efecto y dicho acceso se llevará a cabo con la supervisión de personal autorizado.

MÍA Y LÍA, S.L.U., establece las pautas principales que se deberían cumplir:

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y son, por tanto, protegidas especialmente. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales. Por ello, cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al Responsable de Seguridad y subsana en el menor plazo de tiempo posible.

Existe en la entidad un procedimiento de asignación, distribución y almacenamiento que garantiza la confidencialidad e integridad de las contraseñas.

La asignación de contraseñas se basa en un sistema de perfiles, no siendo las mismas identificables con un usuario. Son, por tanto, contraseñas de acceso limitadas a determinados perfiles.

Existe una relación actualizada de usuarios, con determinación de un perfil de accesos a los recursos, entendidos como sujetos o procesos autorizados para acceder a datos o recursos, que tengan acceso autorizado al sistema de información.

A cada usuario se le comunica su contraseña de acceso por escrito de una contraseña provisional que debe ser renovada en el plazo de 24 horas.

El control de acceso a los sistemas de información lo establece el Responsable de Sistemas de la organización, determinando qué usuarios pueden acceder a los sistemas de información.

Existe una relación de usuarios actualizada con acceso autorizado a cada fichero. Asimismo, se incluye el tipo de acceso o perfil para cada uno de ellos. Esta lista será actualizada puntualmente, en su caso. No se almacenan las contraseñas de acceso, necesitándose volver a ser generadas en caso de olvido.

La periodicidad con la que tienen que ser cambiadas todas las contraseñas existentes en la entidad es 1 vez al año.

Cada uno de los usuarios que se relacionan a continuación accede a los datos de cada uno de los ficheros de la organización, de distinto modo, para el desempeño de sus funciones:

| <b>USUARIOS Y PERFILES DE ACCESO</b>         |                               |  |  |
|--|-------------------------------|--|--|
| <b>Identificación del usuario</b>            | <b>Departamento o sección</b> | <b>Fecha de alta y baja (en su caso)</b> | <b>Derechos concedidos y observaciones</b> |
| 32691228V - PRISCILA DÍAZ BUYO               | DEPARTAMENTO COMERCIAL        | 15/06/2021                               | ACCESO TOTAL A LOS FICHEROS                |
| 32668828L - M <sup>a</sup> ISABEL FOIRA DÍAZ | DEPARTAMENTO COMERCIAL        | 15/06/2021                               | ACCESO TOTAL A LOS FICHEROS                |
| 32696782M - MACARENA VÁZQUEZ PÉREZ           | DEPARTAMENTO COMERCIAL        | 15/06/2021                               | ACCESO TOTAL A LOS FICHEROS                |
| 45430000D - MANUEL ÁNGEL DÍAZ CASANOVA       | DEPARTAMENTO DE DIRECCIÓN     | 15/06/2021                               | ACCESO TOTAL A LOS FICHEROS                |

### **10.3.2 FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS.**

Los ficheros temporales, creados por tiempo determinado, cumplen las mismas medidas de seguridad que se aplican a los ficheros que no tienen ese carácter.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

| <b>FICHEROS TEMPORALES</b>                 |                                   |                              |   |                          |                             |                      |
|--|-----------------------------------|------------------------------|---|--------------------------|-----------------------------|----------------------|
| <b>Identificación del fichero temporal</b> | <b>Datos personales afectados</b> | <b>Ubicación del fichero</b> | <b>Personas autorizadas y nivel de privilegio de acceso</b> | <b>Fecha de creación</b> | <b>Fecha de eliminación</b> | <b>Observaciones</b> |
|  |                                   |                              |   |                          |                             |                      |

### 10.3.3 ACCESOS REMOTOS.

De ser procedente, y en determinados supuestos, se permite al personal autorizado el acceso remoto, a través de redes de comunicaciones, a la base de datos de clientes.

| AUTORIZACIÓN DE ACCESOS REMOTOS |                          |                  |                       |                           |                      |
|---------------------------------|--------------------------|------------------|-----------------------|---------------------------|----------------------|
| Personal autorizado             | Fecha de la autorización | Perfil de acceso | Tipo de acceso remoto | Datos a los que se accede | Medidas de seguridad |
|                                 |                          |                  |                       |                           |                      |

### 10.3.4 TRABAJO CON ACCESO DE DATOS PERSONALES FUERA DE LAS INSTALACIONES DE LA ENTIDAD.

El tratamiento de datos de carácter personal fuera de las instalaciones o locales de ubicación del fichero, incluyéndose el almacenamiento en dispositivos portátiles, tiene que ser expresamente autorizado, de forma previa. En este tratamiento se deberá garantizar el mismo nivel de seguridad que se exige para los tratamientos que se realizan en las propias instalaciones de la entidad, donde están ubicados los ficheros.

| AUTORIZACIONES PARA EL RÉGIMEN DE TRABAJO FUERA DE LAS INSTALACIONES |                      |  |                               |                    |                   |
|--|----------------------|--|-------------------------------|--------------------|-------------------|
| Fichero sobre el que recae la autorización                           | Medidas de Seguridad | Modo de almacenamiento de la información | Usuario (o perfil) autorizado | Periodo de validez | Firma autorizante |
|  |                      |  |                               |                    |                   |

### 10.3.5 ENCARGADOS DE LOS TRATAMIENTOS.

Debido a que existen determinadas entidades encargadas de la prestación de determinados servicios auxiliares (como pueden ser, entre otros, de gestión empresarial, de mantenimiento informático y de gestión técnica de la base de datos, etc.), que les permiten tener acceso a datos de carácter personal, ello hace que exista la necesidad de suscribir con ellas un contrato de prestación de servicios como encargados del tratamiento, conforme al artículo 28 del RGPD.

Todos los contratos se adjuntan al presente Protocolo de seguridad.

| <b>TERCEROS PRETADORES DE SERVICIOS</b> | <b>OBJETO DE LA PRESTACIÓN</b>                   | <b>EXISTENCIA DE CONTRATO ESCRITO</b> |
|---|--|---------------------------------------|
| ACADEMIA A MARIÑA, S.L.                 | consultoría empresarial en protección de datos   | SÍ                                    |
| ASESORÍA J.C. BARREIRO VÁZQUEZ, S.L.    | asesoría laboral, fiscal y contable              | SÍ                                    |
| ARVI SISTEMAS AVANZADOS, S.L.           | soluciones informáticas                          | SÍ                                    |
| VALORA PREVENCIÓN, S.L.                 | asesoramiento en prevención de riesgos laborales | SÍ                                    |

### **10.3.6 COPIAS DE SEGURIDAD, RESPALDO Y PROCEDIMIENTOS DE RECUPERACIÓN. CUMPLIMIENTO DEL ART. 32.1.C) DEL RGPD.**

En cuanto al inventario de activos de información operante y atendiendo a la tipología de datos y a su criticidad, en los que conciernen a copias de los ficheros cuya información esté relacionada con nombres, teléfonos, direcciones de correos electrónicos, fotografías en las que se puedan identificar a las personas, datos bancarios etc., de ser aplicable, la periodicidad de realización de copias de seguridad se determina en una semana (salvo que en dicho período no se hubiera producido ninguna actualización de los datos). Además, se garantizará que los datos puedan ser recuperados de forma previa al momento en el que cualquier incidente o violación de la seguridad pueda acontecer, con el oportuno sistema a implementar que ello lo permita; siendo comprobado éste cada seis meses. De igual modo, si se realizan pruebas para implantar o, en su caso, se hacen modificaciones en los sistemas de seguridad actuantes, se establecerá la incorporación de una adherida y previa copia de seguridad que ello lo permita con las garantías oportunas.

Para el posible caso de tratarse datos relativos a los supuestos recogidos en el art. 9 y/o 10 del RGPD, éstos serán guardados con agregada *backup* en soportes externos respecto a los servidores de los equipos, dispositivos o terminales en los que estén contenidos los mismos, o bien separados del propio centro de actividad para el caso de tratarse de datos en documentación con soporte físico. Incluso podrán ser contratados servicios de guarda y custodia si se considera necesario por motivos de seguridad física. Todo ello en favor del acatamiento del deber de salvaguarda y dando cumplimiento a lo previsto por el art. 32.1.c) del RGPD.

Para los posibles datos de índole digital y, sin ser una lista exhaustiva, podrán ser utilizados alguno o varios de los siguientes dispositivos: cintas magnéticas, discos duros, sistemas *e-cloud*, etc.

### **10.3.7 SOPORTES Y DOCUMENTACIÓN CON DATOS PERSONALES.**

Soporte es todo objeto físico que almacena y/o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y sólo deberán ser accesibles por el personal autorizado.

No obstante, se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, como por ejemplo es el caso de memorias USB; de las que, aunque pueden ser inventariados los soportes, es difícil registrar el contenido exacto en cada momento, debido a los continuos cambios que experimenta.

Los soportes que contengan datos de los ficheros deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del fichero. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier documento que contenga datos personales, deberá procederse a su destrucción física mediante el empleo de una destructora de papel, o bien contratando la tarea de destrucción a alguna empresa especializada que garantice el proceso.

La identificación de los soportes que contengan datos que la entidad considerarse especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensible y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y

documentos identificar su contenido, y que dificulten la identificación para el resto de personas. En el mismo sentido, en el mantenimiento de carpetas en soporte papel con contenido sensible, como por ejemplo nóminas de los trabajadores, la entidad procurará identificar las carpetas mediante etiquetas que no desvelen su contenido para el resto de personas que no tienen autorización de acceso al fichero.

Con todo, y atendiendo a lo anterior, los soportes que contengan datos como consecuencia de *procesos periódicos de respaldo* deberán estar claramente identificados con una etiqueta externa que indique:

- De qué fichero se trata.
- Qué tipo de datos contiene.
- Proceso que los ha originado.
- Fecha de creación.

Cualquier entrada y/o salida de soportes fuera de las instalaciones o locales donde están ubicados los ficheros deberá ser autorizada por el responsable del fichero.

| <b>REGISTRO DE SALIDA DE SOPORTES Y DOCUMENTOS FUERA DE LAS INSTALACIONES</b> |                           |  |                           |                           |                              |
|---|---------------------------|--|---------------------------|---------------------------|------------------------------|
| <b>Fichero sobre el que recae la autorización</b>                             | <b>Contenido concreto</b> | <b>Forma en la que se llevará a cabo</b> | <b>Usuario autorizado</b> | <b>Periodo de validez</b> | <b>Firma del autorizante</b> |
|   |                           |  |                           |                           |                              |

| <b>AUTORIZACIÓN DE SALIDA DE SOPORTES Y DOCUMENTOS</b>    |  |
|---|--|
| <b>Fecha y hora de salida del soporte:</b>                |  |
| <b>SOPORTE</b>  |  |
| <b>Tipo de soporte y número:</b>                          |  |
| <b>Contenido:</b>   |  |
| <b>Procedencia de los datos:</b>                          |  |
| <b>Fecha de creación</b>                                  |  |
| <b>FINALIDAD Y DESTINO</b>                                |  |
| <b>Finalidad:</b>   |  |
| <b>Destino:</b>   |  |
| <b>Nombre/s del /los depositario/s o destinatario /s:</b> |  |
| <b>FORMA DE ENVÍO</b>                                     |  |
| <b>Medio de envío:</b>                                    |  |
| <b>Remitente:</b>   |  |
| <b>Precauciones para el transporte:</b>                   |  |
| <b>AUTORIZACIÓN</b>                                       |  |
| <b>Persona responsable de la entrega:</b>                 |  |
| <b>AUTORIZACIÓN DE SALIDA DE SOPORTES Y DOCUMENTOS</b>    |  |
| <b>Aprobación del responsable de MÍA Y LÍA, S.L.U.</b>    |  |
| <b>Observaciones:</b>                                     |  |
| <b>Firma</b>  |  |

### 10.3.8 INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD.

#### 10.3.8.1 PROCEDIMIENTO DE GESTIÓN Y RESPUESTA.

Se entiende por 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.*

La entidad cuenta con la capacidad de contemplar la existencia de posibles incidencias/incidentes/violaciones de la seguridad (entendido en el presente protocolo como concepto unificado), y así permitir restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de darse tales posibles incidentes físicos o técnicos. Ello de conformidad con lo estipulado en el Reglamento General de Protección de Datos.

Así pues, la entidad puede detectar en qué momento y qué tipo de anomalía se produjo en el sistema lógico y/o físico de la organización, a fin de adoptar las medidas oportunas como respuesta a dicho incidente o violación de la seguridad (inclusive y, en su caso, posibles acciones de notificación, según lo indicado en la información ulterior). En este sentido, mantener un registro de las incidencias, incidentes y violaciones que comprometan o puedan comprometer la seguridad de un tratamiento o fichero y sus datos obrantes, es una labor imprescindible para la prevención y actuación ante posibles ataques a tal seguridad de la información.

La entidad recogerá cuantas incidencias, incidentes y violaciones de la seguridad se pudieran producir sobre los datos que trata. Con tal objeto, a continuación, se establece una lista de incidencias que serán inexcusablemente registradas. Esta lista podrá ser ampliada con otro tipo de incidencias, incidentes y violaciones de la seguridad que pudieran haber quedado omitidas:

| TIPOS DE INCIDENCIAS/INCIDENTES/VIOLACIONES DE LA SEGURIDAD |  |   |
|---|--|---|
| Nº  | TIPO                                   | DESCRIPCIÓN   |
| 1   | Accesos no autorizados                 | Accesos o intentos de accesos a equipos, aplicaciones o ficheros, automatizados o no, sin la debida autorización.                 |
| 2   | Acceso autorizado imposible            | Imposibilidad, por causas diversas, de acceder a un equipo, aplicación o fichero para el que presuntamente se tiene autorización. |
| 3   | Distribución incontrolada              | Se hacen llegar datos de carácter personal a personas no autorizadas.   |
| 4   | Pérdida de datos                       | Pérdida total o parcial de datos de carácter personal de las bases de datos o ficheros.   |
| 5   | Incidencias                            | Irregularidades y /o deficiencias relativas a la resolución de las incidencias, incidentes o violaciones de la seguridad.         |
| 6   | Acceso físico                          | Cualquier violación o situación irregular que pueda afectar a la seguridad de la información en el acceso físico.                 |
| 7   | Recuperación                           | Incidencia en los procesos de recuperación de datos.  |
| 8   | Incidencias a nivel de <i>software</i> | Incidencias o cambios producidos, no comunicados o no autorizados en el <i>software</i> .   |
| 9   | Incidencias a nivel de <i>hardware</i> | Incidencias o cambios producidos, no comunicados o no autorizados en el <i>hardware</i> .   |
| 10  | Soportes                               | Incidencias relativas a deficiencias en el uso, suministro, reutilización o desechado de soportes.                                |
| 11  | Incidencias de comunicaciones          | Aquellas relativas a las redes de comunicaciones.   |

|    |                          |  |
|----|--------------------------|--|
| 12 | Pruebas con datos reales | Pruebas con datos de carácter personal reales.   |
| 13 | Incidencias de cifrado   | Todas aquellas incidencias que se refieran al cifrado de la información.                                       |
| 14 | Otros                    | Todas aquellas incidencias, incidentes y violaciones de la seguridad no contempladas por los tipos anteriores. |

| EJEMPLO DE CLASIFICACIÓN ATENDIENDO AL RIESGO |       |   |
|---|-------|---|
| Nº  | NIVEL | DESCRIPCIÓN   |
|   | ALTO  | Pérdida irrecuperable de datos.                             |
|   |       | Indisponibilidad del sistema por más de [     ] horas.      |
|   |       | Recuperación con incidencia masiva.                         |
|   |       | Revelación de contraseñas a terceros no autorizados.        |
|   |       | Revelación de datos a personal no autorizado.               |
|   |       | Otros.  |
|   | MEDIO | Recuperación con incidencia en otros supuestos.             |
|   |       | Inconsistencias limitadas en la información.                |
|   |       | Indisponibilidad del sistema entre [     ] y [     ] horas. |
|   |       | Otros.  |
|   | BAJO  | Indisponibilidad del sistema por menos de [     ] horas.    |
|   |       | Otros.  |

Con este método de clasificación, podría estipularse la notificación de las violaciones de la seguridad consideradas de nivel “medio” y “alto”.

A continuación, se determina otra agregada forma de valoración y cálculo del riesgo:

**RIESGO = P X I**, siendo **P** el *Volumen* e **I** el resultado de multiplicar la *Tipología* x el *Impacto*.

| VOLUMEN (números de registros completos e identificativos) | VALOR    |
|--|----------|
| Menos de 100 registros                                     | 1        |
| Entre 100 y 999 registros                                  | 2        |
| Entre 1.000 y 99.999 registros                             | 3        |
| <b>Entre 100.000 y 999.999 registros</b>                   | <b>4</b> |
| <b>Más de 1.000.000 registros</b>                          | <b>5</b> |

| TIPOLOGÍA DE DATOS (según GDPR y sector)     | VALOR    |
|--|----------|
| Datos no sensibles                           | 1        |
| <b>Datos sensibles/categorías especiales</b> | <b>2</b> |

| IMPACTO (exposición)                           | VALOR     |
|--|-----------|
| Nulo   | 2         |
| Interno (dentro de la entidad - controlado)    | 4         |
| <b>Externo (perímetro proveedor, atacante)</b> | <b>6</b>  |
| <b>Público (accesible en internet)</b>         | <b>8</b>  |
| <b>Desconocido</b>                             | <b>10</b> |

*Ejemplo: pérdida masiva pública de datos de categorías especiales: 5 x (2x8) = 80 %*

Teniendo en cuenta ahora este segundo método, una posible política de notificación de brechas (violaciones de la seguridad) sería la de notificar cualquier brecha que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo en un umbral superior a 20 (más o menos).
- Ante la coincidencia de dos o más circunstancias cualitativas de las **marcadas en negrita**.

Se podría recomendar comunicar a los interesados cualquier brecha que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo superior a 40 (más o menos).
- Ante la coincidencia de dos o más circunstancias cualitativas de las **marcadas en negrita**.

Todo ello, teniendo presente las estipulaciones contempladas en los arts. 33 y 34 del RGPD.

| ESTADO DE LAS INCIDENCIAS/INCIDENTES/VIOLACIONES DE LA SEGURIDAD |            |   |
|--|------------|---|
| SÍMBOLO  | TIPO       | DESCRIPCIÓN   |
| A  | ABIERTA    | Valor por el que comienzan todas las incidencias.   |
| EP   | EN PROCESO | Estado en que se encontrará durante la tramitación de la incidencia.  |
| C  | CERRADA    | Estado que se produce cuando la incidencia se ha resuelto o cuando se advierte que afecta a otra anterior o posterior que la absorbe, por su propia naturaleza. |

| TIPOS DE RESOLUCIÓN          |   |
|------------------------------|---|
| ESTADO                       | DESCRIPCIÓN   |
| Pendiente                    | Estado por el que comienzan todos los informes, advirtiendo un problema de seguridad.   |
| Resuelto                     | Estado que acontece cuando el problema ha sido solucionado o corregido. En el campo de "Tipo de resolución" se deben incluir la fecha, su estado y la descripción completa. |
| Irreproducible               | No es posible volver a reproducir el problema.  |
| Retrasado                    | Se reconoce la existencia de un problema, pero su resolución se pospone, debiendo indicarse el motivo.  |
| Según el procedimiento       | No se trata realmente de una incidencia. El comportamiento refleja lo afirmado en el procedimiento.   |
| Sin solución técnica         | El problema no puede resolverse por motivos técnicos.   |
| Sin solución                 | El problema no puede resolverse por motivos derivados de la política de la organización.  |
| Anulado por el responsable   | Si el usuario que comunicó la incidencia considera que fue un error, puede solicitar su anulación, decidiendo la persona responsable el paso a este estado.                 |
| Necesidad de más información | Es necesario que el informante de la incidencia aporte más información acerca de ésta.  |

### 10.3.8.2 REGISTRO DE INCIDENCIAS, INCIDENTES Y VIOLACIONES DE LA SEGURIDAD.

|                                   |                      |   |  |
|-----------------------------------|----------------------|---|--|
| <b>NOMBRE DE LA ORGANIZACIÓN:</b> |                      | <b>Incidencia, incidente, violación nº:</b> |  |
|                                   |                      | <b>Fichero:</b>                             |  |
|                                   |                      | <b>RAT vinculado:</b>                       |  |
| Fecha: ___/___/20__               | <b>Hora:</b> ___:___ | <b>Estado (A/EP/C):</b>                     |  |

|   |  |
|---|--|
| Tipo de incidencia:   | <b>Clasificación atendiendo a su riesgo y posible información adicional:</b> |
| Descripción detallada de la incidencia:                     |  |
| Fecha y hora en que se produjo la incidencia:               |  |
| Persona que realiza la comunicación:                        |  |
| Persona/s a quien/es se comunica:                           |  |
| Responsable:  |  |
| Encargado del tratamiento (en su caso):                     |  |
| Delegado de Protección de Datos (en su caso):               |  |
| Efectos que puede producir:                                 |  |
| Tipo de resolución:   |  |
| Procedimiento, medidas correctivas y correctoras aplicadas: |  |
| Persona que ejecuta o supervisa la ejecución:               |  |
| Detalle de los datos restaurados:                           |  |
| Otra información:   |  |

### 10.3.8.3 NOTIFICACIÓN DE VIOLACIONES DE LA SEGURIDAD DE DATOS PERSONALES.

En el supuesto de que el responsable del tratamiento detecte una violación de la seguridad de los datos personales, está obligado a notificarla, sin dilación indebida, a la autoridad de control competente y a más tardar 72 horas después de que haya tenido constancia de ella (artículo 33 del RGPD). Esta obligación no se impone en el caso de que “sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas”. El artículo 34 del RGPD se refiere a la “comunicación de una violación de la seguridad de los datos personales al interesado”.

Para dar operatividad a este apartado en los supuestos que proceda y, completando el mismo, se tendrá presente la *Guía para la gestión y notificación de brechas de seguridad* de la AEPD; especialmente lo determinado como formularios de notificación de incidentes de seguridad (Anexo II) y ejemplos ilustrativos con parámetros, criterios y valores (Anexo III); este último anexo, con el objeto de desarrollar el precedente apartado 10.3.8.1: <https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf>

Para determinar el contenido mínimo que debe incluir la notificación, véase los arts. 33.3 y 34.2 del RGPD en los que se basa la siguiente guía-cuestionario:

| <b>GUÍA-CUESTIONARIO PARA LA NOTIFICACIÓN Y COMUNICACIÓN (EN SU CASO) DE UNA VIOLACIÓN DE LA SEGURIDAD DE DATOS PERSONALES A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y AL INTERESADO</b> |   |               |
|---|---|---------------|
| <b>Posible información antecedente:</b>   |   | <b>Fecha:</b> |
|   |   | <b>Hora:</b>  |
| <b>1</b>  | <b>Descripción de la violación de la seguridad (naturaleza).</b>                              |               |
| <b>2</b>  | <b>Interesados y categorías de datos afectados.</b>   |               |
| <b>3</b>  | <b>Categorías y número de registros de datos personales afectados.</b>                        |               |
| <b>4</b>  | <b>Identificación del Delegado de Protección de Datos (en su caso) o persona de contacto.</b> |               |
|   | <b>Identificación de la persona que detecta la violación de la seguridad.</b>                 |               |

|   |  |   |
|---|--|---|
| 5   | Fecha y hora en la que se ha detectado la violación de la seguridad.   |   |
| 6   | Posibles consecuencias de la violación de la seguridad de datos personales.                                      |   |
| 7   | Medidas propuestas por el responsable del tratamiento como remedio y/o mitigación.                               | Tecnológicas:<br>Organizativas:   |
| 8   | Medidas adoptadas por el responsable del tratamiento como remedio y/o mitigación.                                | Tecnológicas:<br>Organizativas:   |
| 9   | ¿Se trata de una violación de la seguridad de los datos con riesgo para los derechos de los afectados?           | <b>SÍ (Continúa en la cuestión 10).</b><br><b>NO (Continúa en la cuestión 13).</b>  |
| 10  | Autoridad de Control a la que notificar la violación de la seguridad (en su caso).                               | Agencia Española de Protección de Datos   |
| 11  | Fecha y hora de la notificación a la Autoridad de Control (en su caso).  |   |
| 12  | Justificación de la NO notificación de la incidencia en el plazo de 72 horas (en su caso).                       |   |
| 13  | Identificación de la persona que cumplimenta el registro y, en su caso, realiza la notificación de la violación. |   |
| <b>COMUNICACIÓN DE LA VIOLACIÓN DE LA SEGURIDAD AL INTERESADO</b> |  | <b>SÍ (Continúa en la cuestión 15).</b><br><b>NO ES NECESARIO -ART. 34.1 y .3 RGPD- (Continúa en la cuestión 14).</b>   |
| 14  | No es necesario realizar la notificación, en base a lo establecido por el artículo 34.1 y .3 del RGPD:           | -La violación no entraña un alto riesgo para los derechos y libertades de las personas físicas.<br>-Se han adoptado medidas técnicas y organizativas de protección apropiadas sobre los datos afectados por la violación de la seguridad, en particular aquella que hagan ininteligibles los datos personales para personas no autorizadas, como el cifrado.<br>-Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete al alto riesgo para los derechos y libertades del interesado.<br>-Supone un esfuerzo desproporcionado. Si se da este último supuesto, continúa en la cuestión 18. Si no, continúa en la cuestión 19. |
| 15  | Contenido de la notificación (lenguaje claro y sencillo).  | -La naturaleza de la violación de la seguridad de los datos personales.<br>-Nombre y datos de contacto del delegado de protección de datos de la organización.  |

|    |  |   |
|----|--|---|
|    |  | -Una descripción de las posibles consecuencias de la violación de la seguridad.<br>-Una descripción de las medidas adoptadas para corregir la violación o, al menos, mitigar sus efectos. |
| 16 | Fecha y hora de la notificación.   |   |
| 17 | Medio por el que se materializa la notificación.   | Correo electrónico u otro.  |
| 18 | Si la notificación supone un esfuerzo desproporcionado, se deberá justificar el mismo:                                     |   |
|    | Si se opta por una comunicación pública o una medida semejante por la que se informe a los interesados, detallar la misma. | Se ha publicado una nota de prensa informando de la incidencia en el sitio web de la entidad, en el medio y fecha _____.  |
| 19 | Identificación de la persona que cumplimenta el registro y, en su caso, realiza la comunicación de la violación.           |   |

**10.4 PROCESOS Y PROCEDIMIENTOS DE VERIFICACIÓN, EVALUACIÓN Y VALORACIÓN DE LA EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS.**

| 1.- AUDITORÍAS INTERNAS REALIZADAS |                             |                         |                             |  |
|------------------------------------|-----------------------------|-------------------------|-----------------------------|--|
| Fecha                              | Responsable de la auditoría | Alcance de la auditoría | No conformidades detectadas | Medidas correctivas/ correctoras adoptadas |
|                                    |                             |                         |                             |  |
|                                    |                             |                         |                             |  |

| 2.- AUDITORÍAS EXTERNAS REALIZADAS |                             |                         |                             |  |
|------------------------------------|-----------------------------|-------------------------|-----------------------------|--|
| Fecha                              | Responsable de la auditoría | Alcance de la auditoría | No conformidades detectadas | Medidas correctivas/ correctoras adoptadas |
|                                    |                             |                         |                             |  |
|                                    |                             |                         |                             |  |

| 3.- REVISIÓN DE LOS PROCEDIMIENTOS DE COPIAS DE SEGURIDAD |             |                       |                      |
|---|-------------|-----------------------|----------------------|
| Fecha   | Responsable | Revisiones realizadas | Problemas detectados |
|   |             |                       |                      |
|   |             |                       |                      |

| 4.- PERIODICIDAD DE CAMBIOS DE CONTRASEÑAS |                                  |                      |
|--|----------------------------------|----------------------|
| Fecha                                      | Cambios de contraseña realizados | Problemas detectados |
|  |                                  |                      |
|  |                                  |                      |

| 5.- CONTROL ALEATORIO DE ACCESOS POR LOS USUARIOS |                                       |                  |                   |                         |                   |
|---|---------------------------------------|------------------|-------------------|-------------------------|-------------------|
| Fecha responsable y del control aleatorio         | Identificación del usuario verificado | Perfil de acceso | Accesos auditados | Incidencias encontradas | Medidas adoptadas |
|   |                                       |                  |                   |                         |                   |
|   |                                       |                  |                   |                         |                   |

### 10.5 OTRAS MEDIDAS DE SEGURIDAD ADICIONALES.

MÍA Y LÍA, S.L.U. cuenta a mayores con todas las medidas técnicas y organizativas especificadas, y con las siguientes medidas de seguridad adicionales:

- La entidad cuenta con alarma de seguridad instalada por COFERSA SEGURIDAD, S.L.U. Dicha alarma se activa en caso de detectar cualquier tipo de intrusión no deseada.
- El acceso a la documentación física de los archivadores se encuentra restringida, pudiendo acceder solamente el personal del punto anteriormente mencionado.

El artículo 24 del RGPD establece que “teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”. Así pues, conforme a lo contemplado por tal artículo 24, junto a lo indicado por el art. 32.1.d) del mismo reglamento y, teniendo presente el apartado precedente de este protocolo, se ha considerado el establecimiento y la realización de auditorías en materia de protección de datos, preventivamente y entre otros posibles medios de verificación y demostración a ejecutar, como medida técnica apropiada.

Dichas auditorías serían llevadas a cabo con el alcance temporal y material que el Responsable de Seguridad, o en su caso el responsable del tratamiento, estime oportuno. En todo caso, sería de aplicación a los tratamientos llevados a cabo en la entidad, medidas de seguridad implantadas y protocolos de actuación por parte de los empleados; así como afectación al DPD en caso de designación y a los encargados de tratamiento vinculados.

### 11. NECESIDAD DE NOMBRAMIENTO DE DELEGADO DE PROTECCIÓN DE DATOS.

Tal y como señala el artículo 37 del RGPD, el responsable y el encargado del tratamiento están obligados a designar un Delegado de Protección de Datos en los siguientes supuestos:

1. Cuando el tratamiento lo lleve a cabo una autoridad u organismo público. Se exceptúan los tribunales que actúen en ejercicio de su función judicial. De conformidad con lo establecido por el Grupo de Trabajo del art. 29, deberá ser cada Estado miembro el que acote y concrete el concepto en cuestión.
2. Entidades que realizan operaciones de tratamiento a gran escala en determinadas situaciones o afectando a concretas categorías de datos.
  - a. Cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala. Debemos entender por actividades principales aquellas relacionadas con sus actividades primarias y no están relacionados con el tratamiento de datos personales como actividades auxiliares.

- b. Cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de:
- Categorías especiales de datos personales (artículo 9 del RGPD): que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud y vida u orientación sexual de una persona física.
  - Datos relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD.
  - En el resto de los casos, no se exige la designación de un DPD, sino que se determina como potestativo o a determinar en agregadas previsiones. Ello, tal y como señala el artículo 37.4 del RGPD: “En los casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento en asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán de designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El Delegado de Protección de Datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados”.

En consonancia con lo expuesto, el artículo 34 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, clarifica y aumenta el número de supuestos donde se debe nombrar un Delegado de Protección de Datos:

- a) Los colegios profesionales y sus consejos generales.
- b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- f) Los establecimientos financieros de crédito.
- g) Las entidades aseguradoras y reaseguradoras.
- h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

- l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- ñ) Las empresas de seguridad privada.
- o) Las federaciones deportivas cuando traten datos de menores de edad.

A la vista de lo expuesto, en el caso de MÍA Y LÍA, S.L.U. no resultaría necesario el nombramiento del Delegado de Protección Datos. No obstante, esta situación podrá variar en la medida que se realicen nuevos tratamientos de datos, se realicen modificaciones en los tratamientos existentes o la legislación lo exija. En consecuencia, se deberá realizar controles periódicos en aras de detectar estos cambios.

## **12. MODELOS DE DOCUMENTACIÓN PARA EL EJERCICIO DE LOS DERECHOS POR PARTE DE LOS INTERESADOS.**

A continuación, se facilitan los siguientes modelos en favor de poder ejercitar los derechos vinculados a usuarios, interesados y afectados en materia de protección de datos: acceso, portabilidad, rectificación, oposición, supresión y limitación del tratamiento. A mayor abundamiento, en lo que concierne al derecho de información, al derecho a no ser objeto de decisiones individuales automatizadas y a los derechos Schengen, podrá obtener mayor información y, en su caso, acceder a sus correspondientes formularios en <https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos>. Además, a modo de instrucciones, en el mismo link podrá obtener información adicional para dar cumplimiento a los requerimientos precisos para la ejercitación de todos ellos:

### **12.1 MODELO DE EJERCICIO DEL DERECHO DE ACCESO.**

#### **EJERCICIO DEL DERECHO DE ACCESO**

##### **DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... nº ..... C. Postal .....  
Localidad ..... Provincia ..... Comunidad Autónoma .....

##### **DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza .....  
nº....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F....., con correo electrónico ....., por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

##### **SOLICITA**

Que se le facilite gratuitamente el derecho de acceso por ese responsable en el plazo de un mes a contar desde la recepción de esta solicitud, y que se remita, a la dirección arriba indicada, la siguiente información:

- Copia de mis datos personales que son objeto de tratamiento por ese responsable.
- Los fines del tratamiento, así como las categorías de datos personales que se traten.
- Los destinatarios o categorías de destinatarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.

-Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.  
 -El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.  
 -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.  
 -Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.  
 -La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento.  
 -El derecho a presentar una reclamación ante una autoridad de control.  
 En .....a.....de.....de 20.....  
 Firmado:

## 12.2 MODELO DE EJERCICIO DEL DERECHO DE PORTABILIDAD.

**EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS**  
**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**  
 Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza ..... nº ..... C. Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....  
**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**  
 D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F....., con correo electrónico ..... por medio del presente escrito ejerce el derecho de portabilidad de los datos, de conformidad con lo previsto en el artículo 20 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).  
**SOLICITA**  
 Que se le faciliten en el plazo de un mes sus datos personales en un formato estructurado, de uso común y lectura mecánica.  
 En su caso, que los citados datos personales sean transmitidos directamente al responsable ..... (especifíquese nombre o razón social), siempre que sea técnicamente posible.  
 En .....a.....de.....de 20.....  
 Firmado:

## 12.3 MODELO DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN.

**EJERCICIO DERECHO DE RECTIFICACIÓN**  
**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**  
 Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de rectificación: C/Plaza ..... nº ..... C. Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....  
**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**  
 D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F....., con correo electrónico ..... por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).  
**SOLICITA**

Que se proceda a acordar la rectificación de los datos personales, que se realice en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Datos sobre los que solicito el derecho de rectificación:

.....

Que en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Asimismo, en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta rectificación a los mismos.

En .....a.....de.....de 20.....

Firmado:

#### 12.4 MODELO DE EJERCICIO DEL DERECHO DE OPOSICIÓN.

##### EJERCICIO DEL DERECHO DE OPOSICIÓN

###### DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza ..... nº ..... C. Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

###### DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F. ...., con correo electrónico ..... por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

###### SOLICITO

La oposición al tratamiento de mis datos personales, teniendo en consideración que:

El tratamiento de mis datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, debiendo limitarse el tratamiento de los mismos hasta que obtenga respuesta del ejercicio de este derecho.

El tratamiento de mis datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, debiendo limitarse el tratamiento de los mismos hasta que se obtenga respuesta del ejercicio de este derecho.

El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

Sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades (en los dos primeros supuestos), o una misión realizada en interés público (en el tercer supuesto), acredito como situación personal para oponerme al tratamiento de mis datos personales

.....

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado:

#### 12.5 MODELO DE EJERCICIO DEL DERECHO DE SUPRESIÓN (“AL OLVIDO”).

##### EJERCICIO DEL DERECHO DE SUPRESIÓN

###### DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza ..... nº ..... C. Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza ..... nº ....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F....., con correo electrónico ..... por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITA**

Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada.

Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda.

Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta supresión.

En .....a.....de.....de 20.....

Firmado:

**12.6 MODELO DE EJERCICIO DEL DERECHO DE LIMITACIÓN DEL TRATAMIENTO.**

**EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO**

**DATOS DEL RESPONSABLE DEL TRATAMIENTO.**

Nombre / razón social: ..... Dirección de la Oficina /Servicio ante el que se ejercita el derecho de limitación: C/Plaza ..... nº ..... C. Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma .....

**DATOS DEL AFECTADO O REPRESENTANTE LEGAL.**

D./ D<sup>a</sup>. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. .... Comunidad Autónoma ..... con N.I.F....., con correo electrónico ....., por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento UE 2016/679, General de Protección de Datos (RGPD).

**SOLICITO**

Que se limite el tratamiento de mis datos personales, teniendo en consideración:

Que el tratamiento es ilícito y me opongo a su supresión.

Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, y que se comunique esta limitación a cada uno de los destinatarios que ese responsable del tratamiento haya comunicado mis datos personales.

En .....a.....de.....de 20.....

Firmado:

**Nota:** Teniendo en consideración todos los formularios y modelos dispuestos en el presente protocolo y, respecto a su posible utilización y consecuente previa obtención de datos personales, se tendrá presente la inclusión de las oportunas cláusulas de privacidad informativas. Ello cuando fuere preciso de conformidad al deber de informar.

### 13. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD.

El artículo 32.1 del Reglamento General de Protección de Datos, establece que, *teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo*. En el presente caso, se considera pertinente proceder al nombramiento de un Responsable de Seguridad encargado de promover que el tratamiento de los datos personales se realice de conformidad con las medidas previstas por el nuevo Reglamento y la Ley Orgánica estatal y, en concreto, deberá velar por:

- Que los datos sean tratados de manera lícita, leal y transparente.
- Que los datos sean recogidos con fines determinados, explícitos y legítimos, evitando tratamientos ulteriores incompatibles.
- Que los datos recogidos sean adecuados, pertinentes y limitados a los fines para los que son tratados.
- Que los datos recopilados sean exactos y actualizados.
- Que permitan la identificación de los interesados no más tiempo del necesario para los fines en la forma legalmente admisible.

Por otro lado, el Responsable de Seguridad deberá garantizar la seguridad de los datos personales, determinar y proponer las medidas de seguridad a adoptar, así como documentar las actuaciones para demostrar el cumplimiento de la legalidad vigente.

Por lo expuesto, teniendo presente la fecha de inicio de aplicación de este protocolo, recogida en el apartado primero, se procede a nombrar con efecto inmediato a D. MANUEL ÁNGEL DÍAZ CASANOVA, con N.I.F. 45430000D como Responsable de Seguridad. Dicho nombramiento tendrá carácter indefinido, salvo acuerdo de la entidad o renuncia del propio Responsable.

Para que conste a todos los efectos legales, firma la presente.

MANUEL ÁNGEL DÍAZ CASANOVA

REPRESENTANTE LEGAL DE LA ENTIDAD  
(También en favor de la asunción del presente protocolo)

Fdo.-.....

Fdo.- .....

De conformidad con la legislación vigente, dando cumplimiento al deber de información, le comunicamos que el responsable del tratamiento de sus datos personales es MÍA Y LÍA, S.L.U. La finalidad perseguida es el desempeño organizativo y funcional de la entidad en cuestión; siendo base de legitimación, además de posibles ejecuciones contractuales, el consentimiento otorgado, el cumplimiento de obligaciones legales o la satisfacción de intereses legítimos. Informarle que los datos de carácter personal no serán cedidos a terceros salvo por obligación legal o ejecución contractual. Tampoco se contemplan transferencias internacionales. El plazo de conservación de los mismos obedecerá a las exigencias legales operantes. Por otro lado, le informamos de la posibilidad de ejercer los derechos de acceso, rectificación, oposición, supresión, portabilidad y limitación del tratamiento, así como consultar información adicional de protección de datos en [administracion@miaylia.com](mailto:administracion@miaylia.com) o en C/ Real, 105 Bajo (15402 Ferrol).