

laboralrgpd

PROTECCIÓN DE DATOS



Registro de actividades del tratamiento

LUCÍA PIÑERO HERNÁNDEZ

Fecha: 15 de Mayo de 2023

Referencia: REF4D5459344E7A413D

Indice Registro de actividades del tratamiento

Indice Registro de actividades del tratamiento	2
1. Descripción del proyecto	3
I. Promotor del proyecto	3
II. Descripción y objetivo	3
III. Funcionalidades previstas, implantación, sistemas de información y tecnologías	3
2. Identificación y clasificación de los datos	5
3. Identificación de interesados	5
4. Departamentos de la entidad	6
5. Operaciones de tratamiento	7
6. Análisis para necesidad de hacer la EIPD y conclusiones	16
I. Análisis de necesidad	16
1. Análisis de necesidad de las listas de tratamientos previstos en la regulación	16
2. Análisis de la naturaleza, alcance, contexto y fines de tratamiento	16
II. Conclusiones	18
7. Riesgos identificados y medidas de control para riesgos en el tratamiento de nivel bajo	19

1. Descripción del proyecto

I. Promotor del proyecto

Datos Empresa	
Razón social	03908194B - LUCÍA PIÑERO HERNÁNDEZ
Domicilio social	CALLE ROMA, 7 - (45003) TOLEDO
Teléfono	925050198
Email	LUCIAPINERO84@GMAIL.COM

II. Descripción y objetivo

Este es un documento de trabajo orientado a recoger información relacionada con los datos que se tienen que tratar y sobre las operaciones de tratamiento que se quieren llevar a cabo en la entidad, que entren dentro del marco establecido en 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), así como lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

En esta etapa previa a la Evaluación de Impacto de Protección de Datos (EIPD), la información recogida es relevante y contrastada a lo especificado en el RGPD, para determinar si hay un tratamiento de datos de carácter personal, el cual hará obligatoria la realización de una evaluación de impacto. Pero también es útil posteriormente, en la fase de descripción del proyecto y de los flujos de información.

Conviene hacer una breve memoria descriptiva del proyecto, a la cual se puede añadir el resultado de aplicar estas plantillas de recogida de información. Se tienen que identificar y clasificar todos los datos de carácter personal que se prevén tratar. Hay que insistir que aquí se presentan unos modelos de documentos de trabajo orientativos, que se pueden adaptar y mejorar.

III. Funcionalidades previstas, implantación, sistemas de información y tecnologías

Las funcionalidades previstas e implantación son los procedimientos por los que el responsable del tratamiento obtiene y trata los datos de carácter personal.

En este caso, el responsable del tratamiento implementa de manera general, la misma forma de obtención de datos y su posterior tratamiento en los diferentes grupos de afectados, cada uno con una o varias finalidades.

Del mismo modo, los sistemas de información es toda la información recolectada, elaborada, distribuida y almacenada, junto con los procesos que manipulan dicha información y las tecnologías son aquellas mecanizaciones mediante aparatos y procesos de automatización, que soportarán las funciones del sistema de información.

El conjunto es fundamental para minimizar el riesgo de pérdida, alteración, manipulación de los datos de carácter personal tratados por parte del responsable del tratamiento y encargados del tratamiento.

En este punto, se muestra los diferentes sistemas de recogida de datos, de información y tecnologías utilizadas en la entidad:

Manera general de obtener los datos

- Datos personales mediante el uso de cámaras de imágenes o grabaciones.
- En papel por parte de un tutor legal del afectado
- Enviado por correo electrónico por parte de un tutor legal del afectado
- Los facilita el propio interesado mediante cuestionario de papel
- Los facilita el propio interesado mediante cuestionario en página web propia
- Los facilita el propio interesado por correo electrónico
- Los facilita el propio interesado por otro método

Tecnologías utilizadas para el tratamiento utilizadas

Almacenamiento de la información

- Armarios, archivadores, estanterías y/o clasificadores con acceso con llave.
- Armarios, archivadores, estanterías y/o clasificadores con acceso sin llave.
- Base de Datos Local
- Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
- Programa Informatico Local
- Programa Informatico Remoto Externo
- Programa Informatico Remoto Interno
- Servidores externos (nube)

2. Identificación y clasificación de los datos

Según el artículo 4 de RGPD se entiende como 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.

En este apartado listamos los datos personales con el objetivo de minimizar el rango de búsqueda de los mismos:

Datos Personales que tratamos

- Aficiones y estilos de vida
- Características físicas
- Datos bancarios
- Datos no económicos de nomina
- dirección
- dirección email
- DNI
- Fecha de nacimiento
- Firma
- Formación
- Historial del trabajador
- imágenes
- Lengua
- Nacionalidad
- Nombre y apellidos
- Profesión
- Puestos de trabajo
- Salud
- Sexo
- Situación Familiar
- Tarjeta sanitaria
- teléfono
- Titulaciones

3. Identificación de interesados

Este apartado describe a las personas o grupos de personas afectadas por la recopilación y el tratamiento de datos de carácter personal realizado el responsable del tratamiento analizado.

En las operaciones del tratamiento, se verá reflejado el tratamiento que realiza la entidad, recogida de datos y tratamiento en grupo de personas diferenciados en diferentes grupos, cada uno con una o varias finalidades, etc

Los grupos de personas afectadas establecidos por el responsable del fichero son los siguientes:

Afectados

- Clientes
- Niños y sus tutores
- Pacientes
- Personas ajenas
- Potenciales clientes
- Potenciales trabajadores
- Proveedores
- Trabajadores
- Usuarios de la web

4. Departamentos de la entidad

La entidad en su funcionamiento y gestión, depende de una estructura de organización.

Esta organización se refiere a la forma en que se dividen, agrupan y coordinan las actividades de la organización en cuanto a las relaciones entre la dirección y los demás niveles jerárquicos y/o inter-departamentales.

En este apartado especificamos los departamentos de la entidad y personal de cada uno de estos departamentos:

Departamentos
<ul style="list-style-type: none"> • FISIOTERAPIA • OSTEOPATÍA • PILATES TERAPÉUTICO • GIMNASIA HIPOPRESIVA TERAPÉUTICA • ENTRENAMIENTO PERSONAL Y FUNCIONAL TERAPÉUTICO • NUTRICIÓN Y DIETÉTICA • ADMINISTRACIÓN Y DIRECCIÓN

Usuarios Autorizados		
DNI	Nombre	Departamentos
03902819H	BEATRIZ GARCÍA TEMBLEQUE GARCÍA	FISIOTERAPIA, PILATES TERAPÉUTICO, GIMNASIA HIPOPRESIVA TERAPÉUTICA
71220331A	CRISTINA SONEIRA LOPEZ	PILATES TERAPÉUTICO, ENTRENAMIENTO PERSONAL Y FUNCIONAL TERAPÉUTICO

5. Operaciones de tratamiento

Según el artículo 4 del RGPD se entiende como 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.

La identificación de las operaciones de tratamiento que realiza el responsable del tratamiento se realizan mediante los siguientes puntos:

- Nombre del fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- Datos tratados.
- Finalidad o finalidades de los datos recopilados
- El mecanismo de recogida
- El sistema de clasificación y almacenamiento
- Destrucción
- Tecnologías intervinientes
- La previsión de volumen de datos dicha previsión
- Departamento involucrados
- Cesión de transferencia a terceros
- Interesados involucrados en el tratamiento

Apartado 1: Información de los datos	
Actividad Tratamiento:	Empleados TRATAMIENTO DE DATOS PERSONALES DE TRABAJADORES ASALARIADOS
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • DNI • dirección • teléfono • dirección email • Firma • Tarjeta sanitaria • Fecha de nacimiento • Sexo • Nacionalidad • Formación • Titulaciones • Profesión • Puestos de trabajo • Datos no económicos de nomina • Datos bancarios • Situación Familiar • Historial del trabajador
Finalidad:	<ul style="list-style-type: none"> • Mantenimiento de la relación laboral y contra-prestación por los trabajos realizados • Creación de contratos, confección de nóminas y otras tareas relacionadas • Utilización de datos derivados de las actividades de la empresa • Coordinación de actividades empresariales • Archivo/historial de trabajadores y extrabajadores de la empresa • Control y supervisión de la eficiencia y calidad de la entidad • Tramitación de altas y bajas por enfermedad común o accidente laboral • Formación
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario de papel • Los facilita el propio interesado por correo electrónico • Los facilita el propio interesado por otro método
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Armarios, archivadores, estanterías y/o clasificadores con acceso con llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc

Apartado 2: Flujo de datos

- Destrucción:**
- Se destruyen informaticamente con formateo del medio
 - Se destruyen físicamente del medio.

Finalización Tratamiento: Contrato

- Medidas de seguridad implementadas por la entidad:**
- Contraseñas en ordenador
 - Restricción de acceso a zonas
 - Terminales con antivirus
 - Medidas de prevención de pérdida de datos (DLP)

3: Sujetos involucrados

Departamentos:

- ADMINISTRACIÓN Y DIRECCIÓN

Cesión o transferencia:

- Administración tributaria
- Seguridad social
- Bancos y entidades financieras
- Servicio de Prevención de Riesgos Laborales
- Gestoría/Asesoría
- Entidades de Consultoría/Auditoría

Interesados involucrados:

- Trabajadores

Apartado 1: Información de los datos	
Actividad Tratamiento:	Clientes Usuarios de las actividades de Pilates, hipopresiva, y entrenamiento personal y funcional salvo que haya tratamiento de datos de salud, que pasarán a la categoría de pacientes
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • DNI • dirección • teléfono • dirección email • imágenes • Firma • Fecha de nacimiento
Finalidad:	<ul style="list-style-type: none"> • Prestarles un servicio • Gestión contable, administrativa, de facturación, de cobros y pagos • Coordinación de actividades deportivas • Realización de cobro mediante TPV • Control y vigilancia de acceso a lugares
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario de papel • Los facilita el propio interesado por correo electrónico • Los facilita el propio interesado mediante cuestionario en página web propia
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Programa Informatico Remoto Interno • Armarios, archivadores, estanterías y/o clasificadores con acceso con llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc • Servidores externos (nube)
Destrucción:	<ul style="list-style-type: none"> • Se destruyen informaticamente con formateo del medio • Se destruyen físicamente del medio.
Finalizacion Tratamiento:	Contrato
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Terminales con antivirus • Terminales con antimalware • Actualización de sistemas operativos y aplicaciones
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • FISIOTERAPIA • OSTEOPATÍA • PILATES TERAPÉUTICO • GIMNASIA HIPOPRESIVA TERAPÉUTICA • ENTRENAMIENTO PERSONAL Y FUNCIONAL TERAPÉUTICO • NUTRICIÓN Y DIETÉTICA • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • Bancos y entidades financieras • Gestoría/Asesoría • Otros encargados del tratamiento
Interesados involucrados:	<ul style="list-style-type: none"> • Clientes • Potenciales clientes • Usuarios de la web

Apartado 1: Información de los datos	
Actividad Tratamiento:	Curriculums TRATAMIENTO DE DATOS PERSONALES PARA LA SELECCIÓN DE TRABAJADORES ASALARIADOS
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • DNI • dirección • teléfono • dirección email • imágenes • Lengua • Fecha de nacimiento • Nacionalidad • Aficiones y estilos de vida • Formación • Profesión
Finalidad:	<ul style="list-style-type: none"> • Realizar un proceso de selección de personal en función de las capacidades, aptitudes y otros datos de interés incluidos en el currículum • Consultar las referencias de las empresas indicadas en el cv
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario de papel • Los facilita el propio interesado por correo electrónico • Los facilita el propio interesado por otro método
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Armarios, archivadores, estanterías y/o clasificadores con acceso sin llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
Destrucción:	<ul style="list-style-type: none"> • Se destruyen informaticamente con formateo del medio • Se destruyen físicamente del medio.
Finalización Tratamiento:	Indefinido
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Terminales con antivirus • Terminales con antimalware • Copias de seguridad en medios externos
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • No comparto los datos con terceros.
Interesados involucrados:	<ul style="list-style-type: none"> • Potenciales trabajadores

Apartado 1: Información de los datos	
Actividad Tratamiento:	Pacientes TRATAMIENTO DE DATOS PERSONALES DE PACIENTES, SEAN MAYORES O MENORES DE EDAD, QUE RECIBEN TRATAMIENTOS MÉDICOS POR PARTE DE LA EMPRESA

Apartado 1: Información de los datos	
Datos tratados:	<ul style="list-style-type: none"> • Salud • Nombre y apellidos • DNI • dirección • teléfono • dirección email • Firma • Fecha de nacimiento • Sexo • Nacionalidad • Características físicas • Profesión • Puestos de trabajo
Finalidad:	<ul style="list-style-type: none"> • Realización de tratamientos sanitarios • Obtención, desarrollo y almacenamiento del historial clínico del paciente • Realización de certificaciones • Tratamientos de rehabilitación • Realización de cobro mediante TPV • Control y vigilancia de acceso a lugares • Programación de cita
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario de papel • Los facilita el propio interesado por otro método • En papel por parte de un tutor legal del afectado • Los facilita el propio interesado por correo electrónico • Enviado por correo electrónico por parte de un tutor legal del afectado
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Programa Informatico Remoto Interno • Armarios, archivadores, estanterías y/o clasificadores con acceso con llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
Destrucción:	<ul style="list-style-type: none"> • Se destruyen físicamente del medio. • Se destruyen informáticamente con formateo del medio
Finalización Tratamiento:	10 Años
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Armarios con llave u otro elemento de seguridad en la apertura • Terminales con antivirus • Copias de seguridad en medios externos
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • FISIOTERAPIA • OSTEOPATÍA • PILATES TERAPÉUTICO • GIMNASIA HIPOPRESIVA TERAPÉUTICA • ENTRENAMIENTO PERSONAL Y FUNCIONAL TERAPÉUTICO • NUTRICIÓN Y DIETÉTICA
Cesión o transferencia:	<ul style="list-style-type: none"> • No comparto los datos con terceros. • Otros encargados del tratamiento
Interesados involucrados:	<ul style="list-style-type: none"> • Pacientes

Apartado 1: Información de los datos	
Actividad Tratamiento:	Potenciales Clientes TRATAMIENTO DE DATOS PERSONALES DE PERSONAS FÍSICAS QUE QUIEREN RECIBIR INFORMACION SOBRE LOS SERVICIOS O TRATAMIENTOS QUE PRESTA LA ENTIDAD
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • dirección • teléfono • dirección email
Finalidad:	<ul style="list-style-type: none"> • Tramitación de presupuestos • Envío de información comercial de la entidad mediante correo postal, correo electrónico u otros
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado por correo electrónico • Los facilita el propio interesado mediante cuestionario en página web propia • Los facilita el propio interesado por otro método
Clasificación:	<ul style="list-style-type: none"> • Armarios, archivadores, estanterías y/o clasificadores con acceso con llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
Destrucción:	<ul style="list-style-type: none"> • Se destruyen informaticamente con formateo del medio • Se destruyen físicamente del medio.
Finalizacion Tratamiento:	1 Año
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Terminales con antivirus • Terminales con antimalware • Copias de seguridad en medios externos
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • NUTRICIÓN Y DIETÉTICA • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • No comparto los datos con terceros.
Interesados involucrados:	<ul style="list-style-type: none"> • Potenciales clientes

Apartado 1: Información de los datos	
Actividad Tratamiento:	Proveedores TRATAMIENTO DE DATOS PERSONALES DE AUTÓNOMOS O EMPRESAS QUE REALIZAN TRABAJOS Y/O SUMINISTRAN MATERIAL A LA ENTIDAD
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • DNI • dirección • teléfono • dirección email • Firma • Datos bancarios • imágenes
Finalidad:	<ul style="list-style-type: none"> • Gestión contable, administrativa, de facturación, de cobros y pagos • Recepción de la prestación de un servicio • Compra/venta de material • Realizar pedidos
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario de papel • Los facilita el propio interesado por correo electrónico • Los facilita el propio interesado por otro método
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Programa Informatico Remoto Interno • Armarios, archivadores, estanterías y/o clasificadores con acceso con llave. • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
Destrucción:	<ul style="list-style-type: none"> • Se destruyen físicamente del medio. • Se destruyen informáticamente con formateo del medio
Finalización Tratamiento:	Contrato
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Medidas de seguridad locales (alarmas, videovigilancia, etc) • Copias de seguridad en medios externos • Terminales con antivirus • Terminales con antimalware
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • Administración tributaria • Bancos y entidades financieras • Gestoría/Asesoría • Entidades de Consultoría/Auditoría
Interesados involucrados:	<ul style="list-style-type: none"> • Proveedores

Apartado 1: Información de los datos	
Actividad Tratamiento:	Usuarios de la web TRATAMIENTO DE DATOS PERSONALES DE USUARIOS DE LA WEB PARA EL ENVÍO DE INFORMACIÓN SOLICITADO PARA UN SERVICIO Y/O TRATAMIENTO
Datos tratados:	<ul style="list-style-type: none"> • Nombre y apellidos • dirección email • teléfono
Finalidad:	<ul style="list-style-type: none"> • Envío de información comercial de la entidad mediante correo postal, correo electrónico u otros • Programación de cita
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Los facilita el propio interesado mediante cuestionario en página web propia
Clasificación:	<ul style="list-style-type: none"> • Base de Datos Local • Programa Informatico Remoto Interno • Dispositivos externos, discos duros externos, memorias usb, CD's, DVD, etc
Destrucción:	<ul style="list-style-type: none"> • Los datos se sobrescriben informáticamente
Finalizacion Tratamiento:	1 Año
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Terminales con antivirus • Terminales con antimalware • Copias de seguridad en medios externos
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • No comparto los datos con terceros.
Interesados involucrados:	<ul style="list-style-type: none"> • Usuarios de la web

Apartado 1: Información de los datos	
Actividad Tratamiento:	Videovigilancia CÁMARAS UBICADAS EN EL CENTRO PARA PRESERVAR LA SEGURIDAD DE LOS BIENES Y LAS PERSONAS QUE SE ENCUENTRAN EN EL CENTRO
Datos tratados:	<ul style="list-style-type: none"> • imágenes
Finalidad:	<ul style="list-style-type: none"> • Seguridad de la entidad. • Control y supervisión de la eficiencia y calidad de la entidad • Vídeo-vigilancia de instalaciones • Control y vigilancia de acceso a lugares
Apartado 2: Flujo de datos	
Recogida de Datos:	<ul style="list-style-type: none"> • Datos personales mediante el uso de cámaras de imágenes o grabaciones.
Clasificación:	<ul style="list-style-type: none"> • Programa Informatico Local • Programa Informatico Remoto Externo
Destrucción:	<ul style="list-style-type: none"> • Los datos se sobrescriben informáticamente
Finalizacion Tratamiento:	1 Mes
Medidas de seguridad implementadas por la entidad:	<ul style="list-style-type: none"> • Contraseñas en ordenador • Utilización de perfiles con acceso restringido • Contraseñas en aplicaciones específicas • Terminales con antivirus • Terminales con antimalware
3: Sujetos involucrados	
Departamentos:	<ul style="list-style-type: none"> • ADMINISTRACIÓN Y DIRECCIÓN
Cesión o transferencia:	<ul style="list-style-type: none"> • Cuerpos y fuerzas de seguridad del estado
Interesados involucrados:	<ul style="list-style-type: none"> • Clientes • Proveedores • Trabajadores • Potenciales trabajadores • Personas ajenas • Niños y sus tutores • Pacientes

6. Análisis para necesidad de hacer la EIPD y conclusiones

I. Análisis de necesidad

La EIPD no se requiere siempre, en cada actividad de tratamiento, se debe valorar la necesidad de llevarla a acabo o no.

En este punto determinamos si es necesario realizar una EIPD, o no, mediante dos pasos.

1. Análisis de necesidad de las listas de tratamientos previstos en la regulación

La regulación normativa, establece unos supuestos en los cuales obliga, de forma directa, a la realización de una EIPD, estos criterios se pueden dividir en dos subgrupos, en función del punto u artículos que afecte:

Análisis de las listas de tratamiento previstos en la regulación, en los artículos 35.3, 35.4 y 35.5

Elementos a Analizar	Si	No
¿Se lleva a cabo una evaluación sistemática y exhaustiva de aspectos personas de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar?		X
¿Se lleva a cabo tratamiento a gran escala de categorías de datos sensibles?		X
¿Se lleva a cabo tratamiento de datos personales relativos a condenas e infracciones penales?		X
¿El tratamiento implica un control sistemático, monitorización o supervisión a gran escala de áreas de acceso público?		X
¿La empresa realiza algún tipo de tratamiento que esté publicado por la autoridad de control como obligatorio en la realización de la EIPD?		X

2. Análisis de la naturaleza, alcance, contexto y fines de tratamiento

Esta segunda parte se centra en evaluar las características de las actividades de tratamiento a realizar según los aspectos previstos en el artículo 35.1 del RGPD (naturaleza, alcance, contexto y finalidades del tratamiento), mediante las siguientes cuestiones.

El objetivo es clarificar mediante el análisis, si la iniciativa realizada por el área implica tratamiento de datos de carácter personal sujetos al marco jurídico que regula el derecho de protección de datos y valorar si en el tratamiento concurren circunstancias y situaciones que obliguen a la realización de la EIPD:

Sobre cada uno de estos aspectos se deben tener en cuenta las siguientes consideraciones:

Finalidades del tratamiento	Si	No
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala ? Detallar los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala		X
• El número de sujetos afectados: De 0 a 10.000		
• Las categorías de datos tratados: 0 categorías		
• Duración del tratamiento: meses		
• Extensión geográfica del tratamiento: Nacional		
¿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?)		X
¿Se tratan datos identificativos o identificables asociados a: Ideología o opiniones políticas, Afiliación sindical, Religión u opiniones religiosas, Creencias o creencias filosóficas, Origen étnico o racial, Vida sexual u orientación sexual, Datos relativos a salud, Datos de violencia de género o malos tratos, Datos biométricos, Datos genéticos que proporcionan información única sobre la fisiología o la salud del identificado, obtenidos del análisis de una muestra biológica, Datos solicitados para fines policiales sin consentimiento de las personas afectadas, Datos relativos a condenas o delitos penales.	X	
¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?)		X
¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, etc)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿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?		X
¿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, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿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?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
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?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X

Tecnologías empleadas en el tratamiento	Si	No
¿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?		X

Cesiones de datos y transferencias internacionales	Si	No
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?	X	
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control?		X

Percepción de la existencia de riesgo elevado por parte del responsable de la actividad de tratamiento	Si	No
¿Este tratamiento puede conllevar una pérdida o alteración de la información?		X
¿Se utiliza documentación en papel para tratar datos personales?, en tal caso, indicar las medidas aplicadas:	X	
• Se guarda bajo llave: Si		
• Se destruye de forma confidencial: Si		
• Otros: No especificados		

Según los datos obtenidos mediante las diferentes entrevistas y la observación al responsable del tratamiento para la realización del presente informe de análisis de necesidad en relación a la obligatoriedad de realizar una EIPD, cabe destacar que por su naturaleza, alcance, contexto y/o fines en el tratamiento de datos de carácter personal, existen elementos que aumentan sensiblemente el riesgo para los afectados.

II. Conclusiones

En conclusión, según los datos obtenidos del análisis realizado a la entidad y en virtud de lo establecido en el artículo 35 del Reglamento General de Protección de Datos, que establece cuando existen la necesidad de realizar una Evaluación de Impacto relativa a la Protección de los Datos, se requiere al Responsable del Tratamiento hacer una Evaluación de Impacto de Protección de Datos.

7. Riesgos identificados y medidas de control para riesgos en el tratamiento de nivel bajo

El análisis de riesgos para determinar las medidas técnicas y organizativas que garantice los derechos y libertades de los interesados se puede simplificar con un enfoque de mínimos, considerando que el nivel de riesgo al que están expuestas las actividades de tratamiento no es elevado.

El análisis básico de riesgos es un análisis de mínimos que tiene como objetivo simplificar el proceso de análisis de riesgos en aquellas actividades de tratamiento con baja exposición al riesgo.

Los riesgos surgidos en los derechos y libertades de las personas afectadas, valorarán el impacto que puedan tener sobre las mismas, mediante un sistema de probabilidad y consecuencia, y se gestionarán con las medidas técnicas y organizativas apropiadas teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, contexto y fines del tratamiento

Riesgos identificados para un nivel bajo

» **Riesgo para la integridad de los datos personales por modificación o alteración de datos personales de forma no intencionada.**

- *Segregación de funciones mediante la creación de perfiles de acceso*
- *Control de monitorización de amenazas en la red e instalación de antivirus y cortafuegos*

» **Pérdidas borrado no intencionado de datos personales.**

- *Copias de seguridad o utilización de métodos Raid*
- *Almacenamiento en dos ubicaciones diferentes*

» **Falta de confidencialidad en el acceso no autorizado a los datos personales.**

- *Mecanismos de control de acceso mediante la creación de claves de seguridad (contraseñas), que se deberán cambiar cada cierto periodo de tiempo establecido por la empresa.*
- *Segmentación de la red*

» **Violaciones de seguridad por datos no custodiados y sin vigilancia.**

- *Informar y protocolarizar métodos de trabajo*
- *Informar a los interesados*

» **Pérdidas de documentación/datos porque los soportes de almacenamiento no tienen mecanismos que obstaculicen el acceso a personal no autorizado.**

- *Archivo de documentos en lugares seguros, con mecanismos para obstaculizar la apertura a personal no autorizado*

» **Pérdidas de documentación/datos porque no existe un criterio de almacenamiento.**

- *Archivo de documentos bajo un criterio establecido en toda la empresa*

» **Pérdidas de documentación/datos en salida o recepción de soportes.**

- *Creación de procedimientos de entrada y salida de soportes*
- *Encriptación de información en soportes.*

» **Pérdidas de documentación/datos en envíos de datos.**

- *En documentación no automatizada, se realizará mediante procedimiento seguros y/o con encargados del tratamiento certificados y autorizados.*
- *Mediante plataformas de envío automatizadas, se realizará con aplicaciones que cumplan con el RGPD y la LOPDGDD y/o con encargados del tratamiento certificados y autorizados.*

» **Falta de información y legitimación de Videovigilancia.**

- *Informar a todo el personal de la entidad*
- *Colocación de carteles informativos antes del acceso a la de videovigilancia*

- » **Ausencia de procedimientos para el ejercicio de los derechos.**
 - *Creación de procedimientos y canales para el ejercicio de derechos*
 - *Informar a todos los usuarios y encargados del tratamiento sobre los procedimientos en el ejercicio de derechos.*

- » **Ausencia de legitimidad para el tratamiento de datos personales.**
 - *Cláusulas informativas y base legitimadora para el tratamiento de datos personales. Creación y firma de consentimientos*
 - *Informar a los interesados*

- » **Tratamiento ilícito de datos personales.**
 - *Monitorización del uso de datos personales*
 - *Certificación de conductas acordes con el RGPD y la LOPDGDD a los encargados del tratamiento*

- » **No cumplimiento normativo por parte de encargados del tratamiento.**
 - *Firma de contrato e información sobre la política de protección de datos del responsable a los encargados del tratamiento*

- » **No cumplimiento normativo por parte de prestadores de servicio.**
 - *Firma de contrato e información sobre la política de protección de datos del responsable a los encargados del tratamiento.*