



Manual usuario Gestiona RGPD

Abril 2024



ÍNDICE

١.	OBJETO Y ALCANCE DE LA HERRAMIENTA GESTIONA RGPD	4
II.	DESCRIPCIÓN Y USO DE LA APLICACIÓN	4
Α.	Inicio de la Aplicación y consideraciones generales	5
1.	Menú en la cabecera de la página de inicio	8
В.	Introducir nuevo tratamiento de datos Personales o Editar uno existente	11
1.	Cuadros de texto de entrada de datos con formato	12
C.	Gestión de Riesgos: Factores de Riesgo del tratamiento y medidas de mitigación	13
1.	Medidas de mitigación y gestión del riesgo	15
2.	Resultado de la valoración y necesidad de EIPD	21
D.	Finalizar la sesión, guardar datos y salir de la aplicación	25
III.	REFERENCIAS	26

Índice de figuras

FIGURA 1 PANTALLA DE INICIO DE LA APLICACIÓN AL CARGAR LA WEB	5
FIGURA 2 PANTALLA DE INICIO AL CARGAR UN ARCHIVO DE DATOS O INTRODUCIR ALGUNOS TRATAMI	ENTOS
	6
FIGURA 3 DATOS DEL TRATAMIENTO AL DESPLEGARLO EN LA LISTA DE TRATAMIENTOS	7
FIGURA 4 TRATAMIENTOS CARACTERÍSTICOS DE PYMES CONSIDERADOS DE ESCASO RIESGO PARA LOS	QUE
SE PROPORCIONA DOCUMENTOS DE AYUDA	7
FIGURA 5 DESCARGA DE DOCUMENTO DE AYUDA AL SER UN TRATAMIENTO DE ESCASO RIESGO HABIT	UAL EN
PYMES	8
FIGURA 6 MENÚ CABECERA PÁGINA DE INICIO	8
FIGURA 7 MODO OSCURO	9
FIGURA 8 PANEL DE AYUDA	9
FIGURA 9 MENÚ DESPLEGABLE INFORMES/EXPORTAR	10
FIGURA 10 FORMULARIO DE DATOS DE UN TRATAMIENTO	11
FIGURA 11 DATOS DE UN ENCARGADO DEL TRATAMIENTO	12
FIGURA 12 EJEMPLO DEL USO DE TEXTO FORMATEADO EN UN CAMPO DE TEXTO	13
FIGURA 13 PANTALLA GESTIÓN DE RIESGOS: FINALIDADES	14
FIGURA 14 FACTOR DE RIESGO SELECCIONADO. SELECTOR DE MITIGACIÓN ACTIVADO.	14
FIGURA 15 VALORES DEL SELECTOR DE MITIGACIÓN	15
FIGURA 16 EJEMPLO DE UN FACTOR DE RIESGO AÑADIDO POR EL USUARIO	15
FIGURA 17 BOTÓN PARA MOSTRAR LAS TABLAS DE MEDIDAS DE MITIGACIÓN	16
FIGURA 18 BOTONES PARA SELECCIONAR MEDIDAS DE MITIGACIÓN	17
FIGURA 19 OTRA MEDIDA AÑADIDA POR EL USUARIO PARA EL FACTOR DE RIESGO INDICADO.	18
FIGURA 20 MEDIDAS DE SEGURIDAD Y BRECHAS DE DATOS	19
FIGURA 21 MEDIDAS ORGANIZATIVAS Y GOBERNANZA COMUNES	20
FIGURA 22 MEDIDA SELECCIONADA, COLOR DE FONDO DISTINTO	20
FIGURA 23 GESTIÓN DEL RIESGO, RESUMEN Y RESULTADOS	22
FIGURA 24 RIESGO ALTO, EIPD RECOMENDADO	23
FIGURA 25 SE CUMPLE ALGUNA CONDICIÓN DE EIPD OBLIGATORIO	23
FIGURA 26 TABLA RESUMEN	24
FIGURA 27 AYUDA PARA RELLENAR EL JUICIO DE IDONEIDAD	25
FIGURA 28 AVISO AL CERRAR LA PESTAÑA DEL NAVEGADOR	26





I. OBJETO Y ALCANCE DE LA HERRAMIENTA GESTIONA RGPD

GESTIONA RGPD es un recurso de ayuda que no sustituye al responsable en sus decisiones relacionadas con los procesos de gestión del riesgo ni en ninguna de sus decisiones relacionadas con los fines y medios de los tratamientos que lleva a cabo o cualquier otro aspecto del cumplimiento de las normativas de protección de datos personales aplicables a su tratamiento. Por tanto, la herramienta no toma ninguna de las decisiones que corresponden al responsable y encargado del tratamiento, sino que se plantea como un recurso destinado al asesoramiento para las acciones relacionadas con la gestión del riesgo y de los tratamientos de un responsable o un encargado.

La herramienta <u>GESTIONA RGPD</u> ayuda a responsables y encargados a llevar un registro de actividades de tratamiento, identificar gran parte los factores de riesgo para los derechos y libertades de los interesados cuyos datos están presentes en el tratamiento y proponer al responsable o encargado una primera evaluación del riesgo intrínseco, incluyendo la recomendación o la obligación de realizar una EIPD y estimar el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgo específicos. Además, <u>GESTIONA RGPD</u> tiene capacidad para alcanzar estos objetivos con múltiples tratamientos de un mismo responsable.

La herramienta funciona en entorno web y únicamente es necesario tener un navegador para ser utilizada, toda la gestión del tratamiento se realiza en el propio navegador del usuario, sin que se transmitan datos a la Agencia y con total confidencialidad. Durante la sesión de trabajo la información se almacena en la memoria del proceso de ejecución del navegador lo que supone que toda la información se encuentra almacenada en el dispositivo del usuario y el cambio de url, cierre de la pestaña o navegador incluye el borrado de los datos que hubieran sido introducidos en la herramienta. No obstante, la información se puede almacenar en un archivo del ordenador del usuario y recuperar después de cada sesión, permitiendo distintas versiones en diferentes archivos de ordenador.

En ningún caso la utilización de esta herramienta supone la realización de una gestión del riesgo o una EIPD o un cumplimiento de las previsiones de las normas de protección de datos "automático" sino una base sobre la que responsable y encargado podrán apoyarse para garantizar y poder demostrar que el tratamiento es conforme con las previsiones del RGPD. En definitiva, Gestiona RGPD, en su estado de evolución, es el punto de partida para comenzar la gestión del riesgo.

En consecuencia con lo indicado, la mera obtención de los documentos que proporciona la herramienta no supone, en ningún caso, un cumplimiento automático de las obligaciones que el RGPD y la LOPDGDD establecen para los responsables y encargados de los tratamientos de datos personales, en particular lo referido al principio de responsabilidad activa que el RGPD desarrolla en su Capítulo IV. Se trata de documentos iniciales de ayuda orientados a facilitar la comprensión de dichas obligaciones y abordarlas, inicialmente, de forma adecuada.

Este documento guía a los usuarios a través de la interfaz de la aplicación detallando sus funcionalidades y pasos a seguir.

II. DESCRIPCIÓN Y USO DE LA APLICACIÓN

La herramienta se ejecuta en un navegador de internet de manera local (no se transmiten datos por internet y usa la memoria local de ejecución del navegador del usuario). Funciona en cualquier sistema operativo con un navegador actualizado (Windows, Mac OSX, Linux,



Android, iOS). Consta de dos pantallas, la de Inicio, con el conjunto de tratamientos, y la de gestión de riesgos, particular para un tratamiento.

La pantalla de Inicio permite añadir tratamientos, introduciendo la información detallada, (entre la que se incluye la indicada en el Art. 30.1 del RGPD). Muestra los tratamientos gestionados, vuelca los resultados de la evaluación del de riesgos efectuada y permite la generación de informes y el almacenamiento y carga de los tratamientos desde un archivo.

La pantalla de evaluación del riesgo de un tratamiento permite seleccionar los factores de riesgo identificados en el tratamiento, las medidas de mitigación para gestionar el riesgo y calcula una valoración del riesgo intrínseco y residual, así como la recomendación u obligatoriedad de realizar una EIPD.

A. INICIO DE LA APLICACIÓN Y CONSIDERACIONES GENERALES

La aplicación está desarrollada para llevar un registro de los distintos tratamientos efectuados por un único responsable. Si se pretende gestionar tratamientos de distintos responsables, entonces habrá que ejecutar la aplicación para cada uno de ellos y almacenar los datos con la herramienta en archivos distintos.

La aplicación está preparada para gestionar un número elevado de tratamientos, pero ha de tenerse en cuenta que se ejecuta en el navegador del usuario y que es una aplicación web que muestra páginas con un contenido muy extenso, dependiendo por tanto de los recursos del equipo del usuario. Si existe un número considerable de tratamientos y éstos contienen textos muy largos y un elevado número de medidas de mitigación de riesgos, es decir, muchos datos, la representación de las páginas web por parte del navegador puede ralentizarse. De igual manera, la generación de informes puede ser más costosa en tiempo. En estos casos es recomendable separarlos en distintos archivos con menos tratamientos.

Al cargar la página web la aplicación muestra la pantalla de Inicio sin ningún tratamiento de datos. Los tratamientos de datos han de generarse añadiendo nuevos tratamientos con el botón disponible para ello, o bien cargando un archivo de datos previamente guardado con la aplicación.

La pantalla de inicio se divide en tres zonas diferenciadas: cabecera, cuerpo y pie. La cabecera muestra los menús para el uso de la aplicación, el cuerpo muestra los tratamientos y el pie algunas consideraciones para tener en cuenta.

Registro de Tratamientos y Evaluación del Riesgo	1. Cabecera	ېن Castellano English ?) LGuardar کر Cargar 🖨 Informes / Exportar -		
Tratamientos de datos personale	S			
A continuación se relacionan los distintos tipos de tratamie	entos de datos personales:			
Añadir nuevo tratamiento de datos	2. Cuerpo			
 Importante: Recuerde guardar el trabajo en un archivo con el botón g No olvide efectuar las correspondientes copias de seguride Todos los tratamientos corresponden a un único responsa 	3. Pie uardar desde esta pantalla. Al cerrar el navegador e ad del archivo. ble) actualizar la página los datos se pierden.		
Esta herramienta permite la gestión de tratamientos de una entidad en los siguientes aspectos: gestión del Registro de Actividades de Tratamiento, generación del Inventario de Tratamientos (su publicación es obligatorio para las AA.PP) y las bases mínimas para iniciar las actividades de andilisis y gestión de riesgos en el ámbito del RGPD, generación de informes y gestión y almacenamiento local de los datos. Ninguna información ni ninguna copia se transmite o se almacena en la AEPD.				
información ni ninguna copia se transmite o se almacena en la AE	-0.			

Figura 1 Pantalla de inicio de la aplicación al cargar la web



Cuando se han añadido algunos tratamientos o se ha cargado un archivo de datos, entonces la pantalla de inicio muestra los datos del responsable y una lista desplegable con los tratamientos. En el pie se muestran las opciones para crear informes (disponible también en el menú de la cabecera)

Registro de Tratamientos y Evaluación del Riesgo	🕁 Guardar 👌 Cargar 🖨 Informes /
Responsable del Tratamiento	
[Nombre y datos de contacto del Responsable] [NIF]	
[Dirección completa]	
[teléfono] [email]	
[Descripción breve de la actividad desarrollada]	
ejercicio de derechos: [email_ejercicio_derechos]	
[Datos del delegado de protección de datos]	
(Para cambiar estos datos y el DPD edite y modifique el primer tratamiento de la lista)	
Tratamientos de datos personales	
A continuación se relacionan los distintos tipos de tratamientos de datos personales:	
	Exp
Tratamiento 1	
Tratamiento 2	
Tratamiento 3	
Afiadir nuevo tratamiento de datos Generación de informes y exportación Los informes generados tienen carácter de documentos de soporte a la realización de la gestión del riesgo, y en ningún caso sustituy ejecutar por responsables y encargados.	ye, ni reemplaza a las acciones que son nece:
Informe de Registro de Actividades del Tratamiento (Art.30 RGPD) <u>Vista de impresión</u> 🛄 Archivo html 🗋 Archivo doc	
Inventario de Tratamientos (Art 31.2 LOPDGDD) 🔒 <u>Vista de impresión</u> Archivo html DArchivo doc	
Informe extendido de Registro de Actividades de Tratamientos 🔝 Archivo html 🔝 Archivo doc	
Exportar datos a CSV (Excel, etc) [] Archivo csy	

Figura 2 Pantalla de inicio al cargar un archivo de datos o introducir algunos tratamientos

Al desplegar uno de los tratamientos se muestran los detalles de este (la información que se ha introducido en el formulario cuando se ha creado o modificado) junto con el resumen de la evaluación de riesgos en un cuadro a la derecha, en donde también se encuentran sendos botones para editar y modificar los datos del tratamiento o bien eliminarlo.



[...Datos del delegado de protección de datos...]

(Para cambiar estos datos y el DPD edite y modifique el primer tratamiento de la lista)

Tratamientos de datos personales

A continuación se relacionan los distintos tipos de tratamientos de datos personales:

		cxpd
ratamiento 1		
Nombre del Tratamiento	Tratamiento 1	Valoración Riesgo Intrínseco
Descripción del tratamiento	[descripción del tratamiento]	(0.700) Riesgo Medio
Responsable (RGPD)		Valoración Riesgo Residual
Nombre de la empresa Responsable	[Nombre y datos de contacto del Responsable]	🕑 (0.140) Riesgo Bajo
Dirección	[Dirección completa]	Editar/Ver Tratamiento
Actividad que se desarrolla	[Descripción breve de la actividad desarrollada]	
N.I.F.	[NIF]	
Teléfono	[teléfono]	
e-mail	[email]	
e-mail ejercicio de derechos	[email_ejercicio_derechos]	
Corresponsable		
Representante del Responsable	Representante	
Delegado de Protección de Datos	[Datos del delegado de protección de datos]	
Tratamiento de datos per	sonales	
Base legal (1)	Art. 6.1.b) el tratamiento es 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	

Figura 3 Datos del tratamiento al desplegarlo en la lista de tratamientos

Si además el tratamiento se ha indicado como uno de los habituales de escaso riesgo en PYMES y MicroPYMES, en la columna derecha de la vista aparecerá el botón para descargar el archivo de ayuda que proporciona la herramienta que servirá al responsable en su adaptación al RGPD de los tratamientos de datos de clientes, potenciales clientes, empleados, selección de personal, gestión de proveedores y videovigilancia.

Tratamientos característicos en PYMES

Para el caso de que la entidad sea una PYME, se proporciona documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél al que corresponda el presente tratamiento (sólo uno):

1 Más...

- Atención a clientes
- Acciones de captación de potenciales clientes
- Gestión de empleados (RR.HH.)

- Reclutamiento de nuevo personal (RR.HH.)
- Gestión de proveedores
- Seguridad basada en Videovigilancia

Figura 4 Tratamientos característicos de PYMES considerados de escaso riesgo para los que se proporciona documentos de ayuda



V	aloración Riesgo Intrínseco
	🕑 (0.475) Riesgo Bajo
v	aloración Riesgo Residual
	🕑 (0.237) Riesgo Bajo
E	ditar/Ver Tratamiento
A	l ser este tratamiento de Gestión d e
e ri	mpleados (RR.HH.) y de bajo esgo puede descargar las claúsulas
ir	nformativas, las contractuales con
e	ncargados y directrices para el
0	jercicio de derechos de los

Figura 5 Descarga de documento de ayuda al ser un tratamiento de escaso riesgo habitual en PYMES

1. Menú en la cabecera de la página de inicio

En la cabecera de esta página de inicio se muestra un menú en dos líneas.



Figura 6 Menú cabecera página de inicio

En la línea superior aparece un icono con forma de sol o luna para indicar el modo de color que se prefiere para mostrar la página (modo color claro u oscuro) al pulsar sobre él. El modo de color oscuro invierte los colores



Gestiona RGPD	💪 Castellano English 🥐
Registro de Tratamientos y Evaluación del Riesgo	🕁 Guardar 👔 Cargar 🖨 Informes / Exportar 🔹
Responsable del Tratamiento	
[Nombre y datos de contacto del Responsable] [NIF] [Dirección completa] [teléfono] [email] [Descripción breve de la actividad desarrollada] ejercicio de derechos: [email_ejercicio_derechos] [Datos del delegado de protección de datos] (Para cambiar estos datos y el DPD edite y modifique el primer tratamiento de la lista)	
Tratamientos de datos personales	
A continuación se relacionan los distintos tipos de tratamientos de datos personales:	Expandir todos
Tratamiento 1	~
Tratamiento 2	
Tratamiento 3	
Añadir nuevo tratamiento de datos	

Figura 7 Modo oscuro

La siguiente opción es la elección del idioma mostrado, pulsando sobre el deseado. Por último, el icono de la interrogación muestra un panel lateral con una breve ayuda al pulsar sobre él.

Gestiona	×	
Registro de Tratamientos y Evaluad	Instrucciones	
Responsable del Tra	La herramienta se ejecuta en un navegador de internet de manera local (sin conexión a internet).Consta de dos pantallas, la principal con el conjunto de tratamientos, y la de gestión de riesgos, particular para un tratamiento.	
[Nombre y datos de contacto de	Pantalla principal/inicio: Conjunto de Tratamientos	
[Dirección completa] [teléfono] [email]	Permite añadir tratamientos, introduciendo la información detallada, entre la que se incluye la indicada en el Art. 30.1 del RGPD. Muestra los tratamientos gestionados, y vuelca los resultados de la evaluación del de riesgos efectuada.	
 [Descripcion breve de la actividad ejercicio de derechos: [email_ejer [Datos del delegado de protección (Para semblar estes dates y ol DPD) 	Desde esta pantalla podrá almacenar los tratamientos en un archivo (que se descarga con el navegador), y cargarlo posteriormente. También hay un botón para imprimir el informe de registro de actividades (Art. 30.1 RGPD), el inventario (Art 30.2 LOPDGDD) y un informe completo con todos los tratamientos y sus evaluaciones de riesogos (se recomienda modificar los ajustes de impresión del navegador para quitar los márgenes).	
(Para cambiar estos datos y el DPD i	Pantalla Evaluación del riesgo de un tratamientos	
Tratamientos de dat	Tras añadir un nuevo tratamiento, o al seleccionar y editar uno existente, la herramienta mostrará la pantalla para la evaluación del riesgo	
A continuación se relacionan los dis	 Determine, en un primer ciclo de análisis, la aplicabilidad de los diferentes factores de riesgo al tratamiento de datos personales para calcular el riesgo intrínseco. Active para ello cada opción correspondiente (se muestran ejemplos en algunos casos). 	
Tratamiento 1	Para algunos factores de riesgo es necesario indicar también su probabilidad e impacto (un impacto muy significativo supondrá un riesgo alto independientemente de la probabilidad)	l
	• Pulse el menú superior para recorrer las distintas categorías de factores de riesgo. Se recomienda que en un primer análisis se realice un recorrido secuencial.	I.
Tratamiento 2	 En la pestaña "Resultado" obtendrá el nivel de riesgo intrínseco y la valoración sobre la obligación de realizar la EIPD, en un informe resumen.Podrá almacenar los datos en un archivo (que se desarga con el navegador), y cargarlo posteriormente. También hay un botón para imprimir el informe (se recomienda modificar los ajustes de impresión del navegador para quitar los márgenes). 	l
Añadir nuevo tratamiento de date	 Una vez realizada la evaluación del riesgo intrínseco, vuelva al inicio y establezca las medidas y garantías más adecuadas para tratar los riesgos específicos que se han identificado. El botón Medidas para gestionar el riesgo, en el borde inferior de la página, muestra tablas con algunas medidas que pueden ser apropiadas según el concepto y diseño del tratamiento (la selección/deselección se efectúa con un click en la fila de la tabla), y permite introducir otras por el responsable. 	

Figura 8 Panel de ayuda

En la segunda línea de este menú se encuentran los botones para guardar y cargar archivos de datos generados por esta aplicación cuya extensión será siempre ".*aepd*". No utilizar esta extensión impedirá a la herramienta localizar los archivos previamente generados para proceder a su carga o edición.

El botón *Guardar* almacena en un archivo todos los tratamientos y la evaluación de riesgos que se ha hecho con la aplicación y están en la pantalla, en la lista de tratamientos. Los datos están almacenados en la memoria del proceso de ejecución del navegador del usuario y se escriben en un archivo de texto de nombre predefinido



'Tratamientos_de_datos.aepd'. La forma de guardar el archivo mediante el navegador se realiza mediante la descarga local de este.

El botón *Cargar* **borra todos los datos y tratamientos que están en pantalla** y carga en memoria y muestra en pantalla los que se encuentran en el archivo que se selecciona con el explorador de archivos (que ha de ser uno generado previamente con la aplicación).

El botón *Informes/Exportar* muestra un desplegable con las distintas opciones para generar informes:

🕁 Guardar 🔯 Cargar 🕞 Informes / Exportar 🗣
Los informes generados tienen carácter de documentos de soporte a la realización de la gestión del riesgo, y en ningún caso sustituye, ni reemplaza a las acciones que son necesarias ejecutar por responsables y encargados.
Informe de Registro de Actividades del Tratamiento (Art.30 RGPD) 🕞 🛄 🛄
Inventario de Tratamientos (Art 31.2 LOPDGDD) 🕞 🛄 🔝
Informe extendido de Registro de Actividades de Tratamientos 🛄 腕
Exportar datos a CSV (Excel, etc)

Figura 9 Menú desplegable Informes/Exportar

Existen tres tipos de informes según la información que contienen. El Registro de Actividades de Tratamientos recopila la información necesaria de cada tratamiento para cumplir con el Art. 30 del RGPD (datos del responsable, finalidades, interesados, etc). El Inventario de actividades de tratamiento añade al anterior la información correspondiente a la base legal del tratamiento para ser utilizado con fines de transparencia y, por último, el informe extendido que incorpora para cada tratamiento definido por el responsable, la información de la evaluación de Riesgos.

Se ofrece la posibilidad de descargar todos los datos en formato tabla (CSV) para poder ser tratado con aplicaciones del tipo hoja de cálculo.

Los informes pueden obtenerse mediante la vista de impresión del navegador (icono de impresora, que requerirá configurar la impresión con las opciones del navegador); en formato html, que permite almacenar en un archivo la vista del navegador; en formato documento Word/Libreoffice. Al hacer click sobre cada icono se procede a la generación y posterior descarga local del archivo con el informe correspondiente. Los nombres de los archivos con los informes están predefinidos por la aplicación.

Tal como se indicaba al inicio de este capítulo, la generación de informes, en particular la de informe extendido, puede no ser inmediata o tardar algo de tiempo en función de la cantidad de tratamientos y de los datos e información que estos contienen. Téngase en cuenta que toda la información se procesa en el dispositivo del usuario y, por tanto, la agilidad con la que procesa dependerá del volumen de información que sea necesario procesar por el dispositivo, así como de las características específicas de cada dispositivo.



B. INTRODUCIR NUEVO TRATAMIENTO DE DATOS PERSONALES O EDITAR UNO EXISTENTE

Al pulsar el botón *Añadir nuevo tratamiento de datos* al final de la lista de tratamientos, o bien el botón *Editar/Ver Tratamiento* cuando se tiene en la lista uno desplegado, se abre en pantalla un formulario para introducir o modificar todos los datos relevantes y detalles del tratamiento. Algunos de los campos son requeridos y otros opcionales (se muestra un aviso si no se rellena un campo obligatorio).

Identificación del tratamiento	
Nombre para identificar el tratamiento (mávimo 50 caracteres)	
(internet para identificar el tratamiento (internet o caracteres)	
Nombre del Tratamiento	
Breve descripción del tratamiento	
Tratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno):	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél
Iratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno): Más Atención a clientes	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél
Tratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno): Más Atención a clientes Acciones de captación de potenciales clientes	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél Reclutamiento de nuevo personal (RR.HH.) Gestión de proveedores
Tratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno): Más Atención a clientes Acciones de captación de potenciales clientes Gestión de empleados (RR.HH.)	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél Reclutamiento de nuevo personal (RR.HH.) Gestión de proveedores Seguridad basada en Videovigilancia
Iratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno): Más Atención a clientes Acciones de captación de potenciales clientes Gestión de empleados (RR.HH.)	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél Reclutamiento de nuevo personal (RR.HH.) Gestión de proveedores Seguridad basada en Videovigilancia s del tratamiento (Art. 30.1 RGPD)
Tratamientos característicos en PYMES Para el caso de que la entidad sea una PYME, se proporciona que corresponda el presente tratamiento (sólo uno): Más Atención a clientes Acciones de captación de potenciales clientes Gestión de empleados (RR.HH.) Información requerida para el Registro de las actividades Responsable del tratamiento. Art. 4.7 RGPD	a documentos de ayuda para los siguientes tratamientos si el riesgo es bajo. Selecciona aquél Reclutamiento de nuevo personal (RR.HH.) Gestión de proveedores Seguridad basada en Videovigilancia s del tratamiento (Art. 30.1 RGPD)

Figura 10 Formulario de datos de un tratamiento

En el formulario se distinguen los siguientes tipos de datos y detalles para describir un tratamiento:

- Identificación del tratamiento: Nombre y descripción
- Tratamientos de escaso riesgo característicos en PYMES: se contemplan algunos tratamientos de ajo riesgo que son habituales en PYMES. Al marcar uno de ellos la herramienta proporciona un documento de ayuda, que sustituye al documento de ayuda que venía obteniéndose con la herramienta FACILITA_RGPD. La descarga del documento se habilita en la página de inicio al desplegar el tratamiento.
- Información requerida para el Registro de las actividades del tratamiento (Art. 30.1 RGPD):
 - Datos de del responsable, representante, corresponsable y DPD. Los datos de contacto del responsable y del DPD sólo se rellenan o modifican en el primer tratamiento, al ser comunes al resto de tratamientos (gestionados en una sesión o en un archivo cargado/guardado)
 - Licitud del tratamiento (base legal y justificación de ésta)



- Detalles del tratamiento: finalidades, categorías de interesado, datos personales y destinatarios, Información de transferencias internacionales, plazos de supresión y descripción general de medidas de seguridad.
- Otros datos: unidad gestora o interna responsable del tratamiento, información sobre encargados de tratamientos y otra información adicional que se considere necesaria. Al marcar la casilla de existencia de encargados del tratamiento, se muestran campos para incluir sus datos, junto a botones para añadir un nuevo encargado o eliminar el introducido.

la contractionales.		
 Encargado del tratamiento. Art 4.8 RGPD Su organización tiene contratadas terceras empre programas informáticos, proveedor de correo elec videovigilancia u otros que traten o accedan a los 	esas que le prestan servicios como pueden ser los de mantenimiento de su página web, desarrollo de ctrónico, hosting, servicios de prospección comercial/marketing, servicio de limpieza, servicio de s datos por cuenta del responsable.	
Nombre de la empresa		
Dirección encargado	N.I.F.	
$\mathbf{B} \ I \ \underline{\mathbf{U}} \coloneqq \Xi$		
	Teléfono	
Descripción del servicio prestado	Dirección de correo electrónico	
Persona de contacto		
$\mathbf{B} I \underline{\mathbf{U}} \mid \underline{\mathbf{\Xi}} \mid \underline{\mathbf{\Xi}}$		

Figura 11 Datos de un encargado del tratamiento

Una vez rellenados los campos del formulario (se avisa de aquellos requeridos que no se han completado) es necesario pulsar el botón *Guardar cambios y Abrir gestión de riesgos* para que el tratamiento se almacene en la memoria de ejecución del navegador. Una vez almacenado se abre la pantalla de Gestión de Riesgos para el tratamiento, explicado en el epígrafe C.

1. Cuadros de texto de entrada de datos con formato

Los cuadros de texto para introducir datos permiten añadir texto con algunas opciones de formato: negrita, subrayado, cursiva (se pueden combinar) y listas sencillas (no se permiten listas anidadas).

El uso es muy intuitivo y basta con pulsar los botones de la parte superior para activar o desactivar cada opción.



Aunque es posible copiar y pegar texto desde procesadores de texto en los campos de entrada del formulario de la herramienta, y obtener una apariencia correcta en la aplicación, en realidad se están copiando también modificadores de formato que no son visibles para el usuario, lo que puede originar problemas y errores de texto al generar informes Word/LibreOffice. No obstante, la aplicación efectúa un filtrado de algunos modificadores, pero no puede asegurarse que evite totalmente la posibilidad de errores en la generación de ese tipo de informes.

El tamaño de los campos de texto está limitado a un número máximo de caracteres, por lo que si se supera no se podrá incluir más texto o se verá recortado.,

Texto de ejemplo Lista numerada: 1. Elemento 1. Negrita 2. Elemento 2 Lista sin numerar: • Elemento 1, <i>negrita cursiva</i> <u>subrayado</u> • Elemento 2	$\mathbf{B} I \underline{\mathbf{U}} \models \underline{\mathbf{\Xi}}$	
Lista sin numerar: • Elemento 1, <i>negrita cursiva</i> <u>subrayado</u> • Elemento 2	Texto de ejemplo Lista numerada: 1. Elemento 1. Negrita 2. Elemento 2	Î
	Lista sin numerar: • Elemento 1, <i>negrita cursiva</i> <u>subrayado</u> • Elemento 2	-

Figura 12 Ejemplo del uso de texto formateado en un campo de texto

C. GESTIÓN DE RIESGOS: FACTORES DE RIESGO DEL TRATAMIENTO Y MEDIDAS DE MITIGACIÓN

Asesorar al responsable y encargado en el proceso de gestión del riesgo para los derechos y libertades es uno de los principales objetivos de esta herramienta y como resultado del mismo proceso se plantea al responsable y encargado la recomendación o la obligación de llevar a cabo la realización de una EIPD. Para ello, tras guardar los datos en el formulario de alta o edición de un tratamiento se abre una nueva pantalla para este fin.

La pantalla está dividida en dos partes, cabecera y cuerpo.

La cabecera donde se muestra el responsable y nombre identificativo del tratamiento y un menú con las diferentes categorías de factores de riesgo que se contemplan, y el cuerpo donde se realiza la identificación de factores de riesgo atendiendo a la categoría seleccionada.

En la parte derecha de la cabecera se encuentran las opciones para el cambio de modo claro/oscuro, idioma castellano/inglés, panel de ayuda y un botón para volver a la pantalla de inicio de la aplicación con el listado de tratamientos. Al pulsar el botón de inicio, los datos de la gestión de riesgos que se hayan ido seleccionando y modificando se almacenan en la memoria local del navegador.

El cuerpo de la página muestra los distintos factores de riesgo para la categoría seleccionada en el menú de la cabecera con algunos ejemplos (incluyendo la posibilidad de añadir otros ejemplos que no estén contemplados y se consideren el mismo factor de riesgo).

Los selectores permiten indicar aquellos factores de riesgo que son aplicables al tratamiento que se está gestionando. Los valores de riesgo están predeterminados por la herramienta, en algunos casos es necesario también indicar su probabilidad e impacto para determinarlo, es decir, la herramienta sugiere una valoración que puede ser alterada por el responsable o el encargado mediante el selector de mitigación y en base a su criterio como conocedores en detalle de la naturaleza, el alcance, el contexto y los fines del tratamiento.



Gestiona RGPD [Nombre y datos de contacto del Responsable] - Tratamiento 1: Trata [finalidades Tipos Extensión Interesados Técnicas Recogida Efectos I	amiento 1 Responsables Comunicaciones Ot	Castellano English 1. Cabecera ros Seguridad Gestión del Riesgo
Operaciones relacionadas con los fines del tr Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines	r atamiento vinculados al propósito principal.	2. Cuerpo
 Perfilado Creación de perfiles Uso de perfiles Clasificación de individuos Orientación de productos/servicios a individuos o grupos Análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, etc.) Otros 	Mitigación No Mitigado	Mitigado
Evaluación de sujetos Valoración Puntuación Otros	Mitigación No Mitigado	Mitigado
Predicción Inferencia de nuevos datos personales Otros	Mitigación No Mitigado ●	Mitigado
Control del empleado	Mitigación No Mitigado	Medidas para gestionar el riesgo

Figura 13 Pantalla gestión de riesgos: Finalidades

Al seleccionar un factor de riesgo éste se considera aplicable al tratamiento. El selector deslizante de mitigación se activa (con un valor por defecto no mitigado). Este deslizante siempre puede moverse por el usuario por los distintos valores en función del análisis que se haya realizado. No obstante, la herramienta lo mueve automáticamente cuando se seleccionan medidas de mitigación.

Finalidades Tipos Extensión Interesados Técnicas R	ogida Efectos Responsable	Comunicaciones Otros	Seguridad	Gestión del Riesgo
Identificadores únicos	Mitig	ación		
● IP	No M	tigado	Mitigado	
MAC	•			
IMSI o IMEI		lo mitigado		
ID de un dispositivo		10 miligado		
N. teléfono				
DNI, NIE, N. Pasaporte o equivalente				
N. de la Seguridad social				
Matrícula de vehículo				
Número de tarjeta de crédito.				
UID				
 Otros 				

Figura 14 Factor de riesgo seleccionado. Selector de mitigación activado.

Los posibles valores que la aplicación considera en relación con el factor de mitigación son los indicados en la siguiente figura: *No mitigado, Limitadamente mitigado, significativamente mitigado* y *Totalmente mitigado*.



Figura 15 Valores del selector de mitigación

La herramienta permite añadir otros factores de riesgo que no contempla, pestaña Otros, para los cuales es necesario indicar mediante selectores deslizantes la probabilidad e impacto para así calcular el riesgo (máximo cuando la probabilidad sea muy alta y el impacto muy significativo, y mínimo cuando sea improbable y con impacto muy limitado), tal como se muestra como ejemplo en la siguiente figura:

Gestiona RGPD	ratamiento 1: Tratamiento 1		🔆 Castellan	no English	?
Finalidades Tipos Extensión Interesados Técnicas Re	ecogida Efectos Responsables Comunicacio	ones Otros Seguridad G	estión del Riesgo	INICIO	
Otros factores de riesgo específic	os del tratamiento				
s necesario estudiar las peculiaridades del tratamiento para esarrollo. El responsable de llevar a cabo el análisis de riesc	a identificar factores de riesgo para los derechos gos ha de realizar un análisis crítico de su tratam	s y libertades que no estén io niento para señalar aquellas :	lentificados explícitamente e situaciones singulares que p	en el RGPD o en odrían tener afe	su ctación
esde el punto de vista de los riesgos introducidos. En partic	cular, los identificados en los códigos de conduc	cta a los que se está adherid	o a los esquemas de certifica	ación.	ctación
rde el punto de vista de los riesgos introducidos. En partic	cular, los identificados en los códigos de conduc Probabilidad	cta a los que se está adherid	o a los esquemas de certifica Mitigación	ación.	
sde el punto de vista de los riesgos introducidos. En partic Factor de riesgo 1 Introducir factor de riesgo Ejemplo	cular, los identificados en los códigos de conduc Probabilidad Improbable	cta a los que se está adherid Muy alta	o a los esquemas de certifica Mitigación No Mitigado	ación. Mitig	jado
sde el punto de vista de los riesgos introducidos. En partic Factor de riesgo 1 Introducir factor de riesgo Ejemplo Aplica	cular, los identificados en los códigos de conduc Probabilidad Improbable Baja	cta a los que se está adherid Muy alta	o a los esquemas de certifica Mitigación No Mitigado	ación. Mitig gado	gado
sde el punto de vista de los riesgos introducidos. En partic Factor de riesgo 1 Introducir factor de riesgo Ejemplo Aplica	cular, los identificados en los códigos de conduc Probabilidad Improbable Baja Impacto	cta a los que se está adherid Muy alta	o a los esquemas de certifica Mitigación No Mitigado	ación. Miti <u>c</u> jado	gado
esde el punto de vista de los riesgos introducidos. En partic Factor de riesgo 1 Introducir factor de riesgo Ejemplo Aplica	cular, los identificados en los códigos de conduc Probabilidad Improbable Baja Impacto Muy limitado	cta a los que se está adherid Muy alta Muy significativo	o a los esquemas de certifica Mitigación No Mitigado A Limitadamente mitic	ación. Mitig	gado

Figura 16 ejemplo de un factor de riesgo añadido por el usuario

En una primera fase de la gestión de riesgos se trata de ir seleccionando en el menú cada categoría de factor de riesgo e ir señalando aquellos que son aplicables al tratamiento, para proseguir posteriormente con la fase de mitigación y gestión del riesgo, como se describe en el siguiente epígrafe.

Los factores de riesgo desplegados en esta herramienta no tienen carácter exhaustivo, sino de mínimos, y el responsable deberá identificar aquellos que sean específicos para el tratamiento e incluirlos en su evaluación atendiendo a la naturaleza, el ámbito o alcance, el contexto y los fines específicos del tratamiento de datos personales.

1. Medidas de mitigación y gestión del riesgo

La herramienta propone algunas medidas para gestionar los riesgos del tratamiento. Se proponen distintas medidas asociadas a los distintos factores de riesgo que se han seleccionado, que pueden ser comunes a varios factores de riesgo. Se permite también añadir nuevas medidas definidas por el usuario.

Las medidas propuestas por la herramienta se clasifican en las siguientes dimensiones:

 a) Concepto y diseño del tratamiento y Protección de datos desde el diseño: Asociados a las operaciones del tratamiento, por tanto, a las categorías del menú



superior Finalidades, Tipos, Extensión, Interesados, Técnicas, Recogida, Efectos, Responsables, Comunicaciones y Otros.

- b) Seguridad, fallos, errores y gestión de brechas: Para las medidas de seguridad se recomiendan como orientación las medidas del Esquema Nacional de Seguridad (ENS) (haciendo corresponder la categoría ENS con el nivel de riesgo del tratamiento). Hay que tener en cuenta que, aunque no se seleccione factores de riesgo del menú Seguridad, han de establecerse medidas de seguridad y gestión de brechas.
- c) Medidas de gobernanza y políticas de protección de datos: conjunto de medidas que podrían implementarse al desplegar políticas de protección de datos como parte de la gobernanza del tratamiento (medidas comunes a las específicas para el tratamiento y las establecidas como parte de la gobernanza de la organización)

La selección de las medidas puede realizarse de dos maneras:

 En cada pantalla correspondiente al menú superior con las categorías de factores de riesgo, mediante el botón *Medidas para gestionar el riesgo* en el borde inferior derecho de la página. Se mostrará una tabla con las medidas de la dimensión a) definida en el párrafo anterior y dimensión b) en la categoría de factores de riesgo Seguridad.

Gestiona RGPD [Nombre y datos de contacto del Responsable] - Tratamient Finalidades Tipos Extensión Interesados Técnicas Recogida	to 1: Tratamiento 1 Efectos Responsables C	omunicaciones Otrc	读 Castellano English ? 《 Inicio os Seguridad Gestión del Riesgo
Identificadores únicos	Mitigación		
IP IP	No Mitigado	Mitigado	
MAC			
IMSI o IMEI		iti	
ID de un dispositivo	Limitadamente m	hitigado	
N. teléfono			
DNI, NIE, N. Pasaporte o equivalente			
N. de la Seguridad social			
Matrícula de vehículo			
Número de tarjeta de crédito.			
UID UID			
Otros			
Datos y metadatos de las comunicaciones electrónicas	Mitigación		
Correos electrónicos	No Mitigado	Mitigado	
Mensajes instantáneos	•		Mostrar y seleccionar
Llamadas de teléfonos			medidas de
Videollamadas			mitigación/control
Otros			Medidas para gestionar el riesgo

Figura 17 Botón para mostrar las tablas de medidas de mitigación

En la pantalla correspondiente al menú superior *Gestión del riesgo*, donde pueden seleccionarse las medidas correspondientes a las tres dimensiones a), b) y c) definidas anteriormente. Se encuentra después de la tabla resumen del tratamiento:



	Gestic	ona RGPD	×	Castellano	English	?
[Nombre	y datos de conte	acto del Responsable] - Tratamiento 1: Tratamiento 1		🖄 Ini	icio	
Finalidades	Tipos Extensió	n Interesados Técnicas Recogida Efectos Responsables Comunicaciones Otros Segurida Gestión	del Riesg	9		
Proced	imiento de	gestión para reducir el riesgo				
Para cada f siga los sig	factor de riesgo, e juientes pasos:	s necesario seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades d	e los inter	esados. Para ay	udar a su se	lección
Los listados afrontando	s de medidas que : las peculiaridade	ie pueden seleccionar no son exhaustivos, ni obligatorios, ni de medidas mínimas, sino ilustrativos. El responsable o s concretas de su tratamiento	encargado	> han de gestio	nar el riesgo	1
		Medidas de mitigación asociadas a determinados factores de riesgo				
	Paso 1	Según el factor de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comu riesgo.	nes a otro	s factores de		
		Mostrar medidas				
					_	
		Medidas de gestión de brechas de datos personales y seguridad de los datos para libertades de las personas físicas	os dere	chos y		
	Paso 2	Han de establecerse controles específicos orientados a garantizar una correcta detección y gestión de brec Para proteger la seguridad de los datos para los derechos y libertades de las personas físicas, se recomienc en el ENS, ampliando a medidas para garantizar la resiliencia, así como para prevenir los fallos y errores en protección de datos y aplicaciones.	has de da la el criter las garant	tos personales. io establecido tías de		
		Mostrar medidas				
					_	
		Medidas de mitigación organizativas, de gobernanza y políticas de protección de d	atos			
	Paso 3	Medidas generales y comunes para todos los factores de riesgo. En función del nivel de riesgo del tratamie exigente con estas medidas.	ento se hal	orá de ser más		
		Mostrar medidas				

Figura 18 Botones para seleccionar medidas de mitigación

Al pulsar el botón Medidas para gestionar el riesgo, en cualquiera de los casos anteriores, se muestra una tabla, con algunas diferencias según se trate de las dimensiones **a**), **b**) y **c**).

a) Concepto y diseño del tratamiento y Protección de datos desde el diseño:

La ventana emergente que se muestra contiene tres partes diferenciadas:

La primera presenta una tabla con las medidas de mitigación o gestión del riesgo que la herramienta proporciona de manera predeterminada para los factores de riesgo (operaciones del tratamiento) que se han seleccionado.

La segunda muestra una tabla con el resto de las medidas que proporciona la herramienta, asociadas de manera predeterminada a otros factores de riesgo no seleccionados, pero que el responsable del tratamiento puede considerar adecuadas también.

Por último, para cada factor de riesgo que se ha seleccionado se ofrece la posibilidad de añadir nuevas medidas. Es necesario pulsar el botón *Añadir* para que se guarde (pudiéndose editar o eliminar posteriormente)



.

Otras medidas aplicadas:

Jentificadores unicos					
Otra medida añadida por el responsable	» 💼				
Introducir medida de control/mitigación para: Identificadores únicos	Añadir				

Figura 19 Otra medida añadida por el usuario para el factor de riesgo indicado.

Las tablas tienen dos columnas, factor de riesgo (operación del tratamiento) y descripción de las medidas, por orden alfabético y con un cuadro de búsqueda.

	actions	PCDD						
Procedimiento d	e gestión para	a reducir el ries	sgo					\times
A continuación se mu responsable o encarg Seleccionar o introduc	uestra un listado de ado han de gestio <i>:ir medidas (por de</i> j	e medidas y garan onar el riesgo afror efecto se establece i	tías que podrían a ntando las peculiar un determinado niv	doptarse para gesti idades concretas de vel de mitigación, qu	onar el riesgo, no es exh e su tratamiento. e también ha de revisar:	austivo, ni o se)	obligatorio, ni de mínimos. El	
Las medidas se han e	xtraído de la guía j	publicada por la A	EPD <u>"Gestión del i</u>	riesgo y evaluación	de impacto en tratamier	ntos de dato	os personales"	
Operación	Descripción	Q Buscar				1		Â
ldentificadores únicos	Aislar y segregar traten datos pers	fases del tratamie sonales (p.ej. datos	nto entre sí para q anonimizados) o	ue traten datos de u recurriendo a su seu	una forma más limitada. Idonimización.	Por ejemplo	o haciendo que algunas fases no	Ū
ldentificadores únicos	Anonimización te	emprana de los da	tos					
ldentificadores únicos	Aplicar otras técn	nicas de privacidad	l desde el diseño e	en el tratamiento de	datos personales			
Resto de medida	is de control y	mitigación dis	sponibles					
Operación		Descripción	Q Buscar			2		Ô
Comunicaciones		Caducidad y reini	icio periódico los i	dentificadores único	s			
Comunicaciones		Cambio de las ele	ecciones técnicas p	oara implementar el	tratamiento para evitar	la falta de ti	ransparencia.	
Comunicaciones		Dar al interesado	la capacidad de p	resentar objeccione	s previas a las transferer	ncias.		
Comunicaciones		Desvinculación d	el identificador co	n otros identificadoi	es			
Comunicaciones		Exigir una acción	positiva e informa	ida del usuario para	la emisión de identifica	dores único:	s.	-
Otras medidas	aplicadas:							
ldentificadores ún	icos					3		
Introducir medid	a de control/mitiga	ación para: Identif	icadores únicos				Añadir	

b) Seguridad, fallos, errores y gestión de brechas:

Este tipo de medidas son siempre necesarias, aunque no se seleccione ningún factor de riesgo de la categoría *Seguridad*. Por eso la tabla que se muestra contiene todas las medidas disponibles por la herramienta. Si se ha seleccionado alguno de los factores de riesgo de *Seguridad* como aplicable al tratamiento, de manera análoga al caso a) anterior la herramienta ofrecerá la posibilidad de añadir nuevas medidas.



Las tablas tienen cuatro columnas, según el documento de origen, el tipo de medida, la referencia ENS cuando aplica y la descripción de las medidas, por orden alfabético y con un cuadro de búsqueda.

Procedimiento	de gestión para rec	ducir el ri	esgo	×		
A continuación se muestra un listado de medidas y garantías que podrían adoptarse para gestionar el riesgo, no es exhaustivo, ni obligatorio, ni de mínimos. El responsable o encargado han de gestionar el riesgo afrontando las peculiaridades concretas de su tratamiento.						
Seleccionar o intro	ducir medidas (por defecto	o se establec	e un determinado nivel de mitigación, que también ha de revisarse)			
Las medidas se ha sobre el riesgo de	n extraído de las guías pu brechas masivas en AA.Pl	ıblicadas po <u>P."</u> , y el <u>"Esq</u>	r la AEPD <u>"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", "Orientaciones</u> uema Nacional de Seguridad (ENS) <u>"</u>			
NOTA: En tratamie activos necesarios seguridad del siste gestión de brechas	ntos que no están someti para dar soporte al tratar ema equivalente al nivel d s de datos personales	idos a la obl niento en ca le riesgo del	igación del ENS, se tendrán que implementar las medidas necesarias para gestionar el nivel de riesgo de los ida una de sus fases. Se recomienda emplear al menos las medidas indicadas en el ENS para la categoría de tratamiento obtenido con esta herramienta, junto con las medidas de control para garantizar la detección y			
Origen	Tipo	Ref.	Descripción Q Buscar	*		
ENS	Medidas de protección	ENS mp.s.3	Protección de los servicios: Protección de la navegación web			
ENS	Medidas de protección	ENS mp.s.4	Protección de los servicios: Protección frente a denegación de servicio			
Guía Gestión del Riesgo	Gestión de brechas de datos personales		Planes de contingencia ante una brecha de datos personales.			
Guía Gestión del Riesgo	Gestión de brechas de datos personales		Establecimiento de medios técnicos para la detección automática de brechas de datos personales.			
Guía Gestión del Riesgo	Gestión de brechas de datos personales		Herramientas de gestión de incidentes adaptadas a los requisitos del RGPD.			
Otras medid	as aplicadas:			•		
			Ace	ptar		

Figura 20 Medidas de Seguridad y Brechas de Datos

c) Medidas de gobernanza y políticas de protección de datos:

Estas medidas son generales y comunes de la organización para todos los tratamientos, por eso la selección está habilitada únicamente cuando se está gestionando el primer tratamiento de la lista de tratamientos en la página de Inicio. Se muestra la tabla únicamente en el menú superior *Gestión del Riesgo*.

La tabla tiene dos columnas, con el tipo y descripción de las medidas, por orden alfabético y con un cuadro de búsqueda. También ofrece la opción de añadir nuevas medidas por el usuario.



Ť.

Procedimiento de ge	estión para reducir el riesgo	~
A continuación se muestra responsable o encargado h	i un listado de medidas y garantías que podrían adoptarse para gestionar el riesgo, no es exhaustivo, ni obligatorio, ni de mínimos. El han de gestionar el riesgo afrontando las peculiaridades concretas de su tratamiento.	
Seleccionar o introducir me	edidas (por defecto se establece un determinado nivel de mitigación, que también ha de revisarse)	
Las medidas se han extraíd	do de la guía publicada por la AEPD <u>"Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"</u>	
Seleccionarlas en el prim	er tratamiento, al ser medidas organizativas, comunes para todos los tratamientos	
Тіро	Descripción Q Buscar	
Marco de gobernanza	Existe un mandato y compromiso concreto de la dirección de la organización con relación a la gestión del riesgo para los derechos y libertades de los interesados.	
Marco de gobernanza	Está integrada la gestión del riesgo para los derechos y libertades de los interesados en los procesos de gestión de la organización.	
Marco de gobernanza	Existe una referencia explícita a la política de gestión del riesgo para los derechos y libertades en el marco de gestión del riesgo de la organización.	
Marco de gobernanza	Están diferenciadas las medidas que implementan las políticas de gestión de riesgos para los derechos y libertades de las políticas de gestión del riesgo de cumplimiento, legal o del riesgo de responsabilidad civil y penal.	
Marco de gobernanza	Están definidos los roles y asignación de responsabilidades y recursos necesarios para garantizar la protección de datos en la organización.	
Marco de gobernanza	Existen los recursos necesarios para garantizar la protección de datos en la organización.	
Otras medidas apli organizativas, políticas (cadas: de protección de datos	•
Introducir medida de o	control/mitigación organizativa	
	Acepta	r

Figura 21 Medidas organizativas y gobernanza comunes

Para seleccionar una medida basta con hacer click en la fila de la tabla, cambiando entonces el color de fondo de la fila (para deseleccionarla basta con hacer click de nuevo con el ratón). Al seleccionar medidas en las tablas propuestas, la herramienta considera un nivel de mitigación por defecto (moviendo automáticamente los selectores deslizantes de mitigación), aunque el responsable ha de gestionar afrontando las peculiaridades concretas de su tratamiento.

Procedimiento	de gestión para reducir el riesgo	\times
A continuación se r responsable o enca	nuestra un listado de medidas y garantías que podrían adoptarse para gestionar el riesgo, no es exhaustivo, ni obligatorio, ni de mínimos. El Irgado han de gestionar el riesgo afrontando las peculiaridades concretas de su tratamiento.	
Seleccionar o introd	lucir medidas (por defecto se establece un determinado nivel de mitigación, que también ha de revisarse)	
Las medidas se har	extraído de la guía publicada por la AEPD "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales"	
Operación	Descripción Q Buscar	1
ldentificadores únicos	Anonimización temprana de los datos	
Identificadores únicos	Aplicar otras técnicas de privacidad desde el diseño en el tratamiento de datos personales	
ldentificadores únicos	Aplicar técnicas de privacidad diferencial en el acceso a datos personales	
ldentificadores únicos	Cancelación en las primeras fases del tratamiento de algunas categorías de datos	





Al cerrar la ventana emergente o al pulsar el botón aceptar (esquina superior derecha e inferior derecha respectivamente), las medidas de mitigación seleccionadas y añadidas se guardan en la memoria local del navegador y se efectúan los cálculos pertinentes de la Gestión del Riesgo.

La valoración del nivel de riesgo para cada factor que efectúa la herramienta, así como el cálculo final de nivel de riesgo, tiene carácter general y supone una evaluación mínima que, en su caso, tendrá que ser ajustada por el responsable para determinar el nivel de riesgo del tratamiento con precisión.

2. Resultado de la valoración y necesidad de EIPD

El menú superior *Gestión del Riesgo* muestra una página extensa con tres partes diferenciadas:

- Valoración del riesgo y necesidad de EIPD y resumen de factores de riesgo identificados y medidas aplicadas. La necesidad de EIPD se evalúa según los criterios señalados en el RGPD, EDPB y AEPD (Art. 35 RGPD)
- Selección de medidas de mitigación asociadas a los factores de riesgo, de seguridad y brechas de datos, organizativas, de gobernanza y políticas de protección de datos (ya visto en el punto anterior)
- Evaluación de la necesidad y proporcionalidad del tratamiento. Se muestran campos para rellenar con los correspondientes juicios de idoneidad, necesidad y proporcionalidad. Estos datos se guardan en la memoria local del navegador cuando se pulsa el botón *Inicio*.



	el tratamiento : Tratamiento 1
/04/2024	
loración Riesgo Intrínseco	Valoración Riesgo Residual
🕑 (0.475) Riesgo Bajo	🔮 (0.237) Riesgo Bajo
Fuentes de riesgo identificadas	lagrupadas por categorías):
Finalidades	No se han especificado factores de riesgo
Tipos	Identificadores únicos - Mitigación: Limitadamente mitigado Medidas de mitigación/control
	- Aplicar otras técnicas de privacidad desde el diseño en el tratamiento de datos personales
	- Otra medida añadida por el responsable
Extensión	No se han especificado factores de riesgo
Interesados	No se han especificado factores de riesgo
Recogida	No se nan especificado factores de riesgo No ra han argarificado factores da riesgo
Efectos	No se han especificado factores de riesgo
Responsables	No se han especificado factores de riesgo
Comunicaciones	No se han especificado factores de riesgo
Otros	No se han especificado factores de riesgo
Seguridad	No se han especificado factores de riesgo Medidas de mitigación/control
	- (ENS org.1) Política de seguridad
	- (ENS org.2) Normativa de seguridad - (ENS op.pl.3) Planificación: Adquisición de nuevos componentes
Otras medidas de mitigación/co	ntrol seleccionadas para los factores de riesgo cifrado en reposo y desde el resoansable (ZKP, homomórfico,)
Medidas de mitigación organi	tativas, de gobernanza y políticas de protección de datos
 Políticas en los procedimientos: de tratamiento el requerir inform 	Están incluidos en los procedimientos de adquisición de productos, sistemas o servicios que van a implementar operaciones dentro de la actividad nación y garantías para asegurar y poder demostrar que dicho tratamiento cumple con el RGPD.
Procedimiento de ges ara cada factor de riesgo, es nece iga los siguientes pasos: os listados de metilas que se pue frontando las peculiaridades conc	tión para reducir el riesgo sario seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son exhaustivos, ni obligatorios, ni de medidas minimas, sino illustrativos. El responsable o encorgodo han de gestionar el riesgo retas de su bratamiento Medidas de mitigación asociadas a determinados factores de riesgo Bigin el fictor de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comuner a otros factores de
Procedimiento de ges Pras cada factor de riesgo, es nece las los lajuientes pasos: los talatos de meditas que se pue difontando las peculiaridades conc Paso 1	tión para reducir el riesgo stato seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son exhaustivos, ri obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encorgodo han de gestionar el riesgo medidas de mitigación asociadas a determinados factores de riesgo Siguin a táctor de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de neego. Modirar medidar Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas físicas 'uno de estibuerene controles regueixínes o dentados a garantiar una correct detección y pesitín de brechas de datos personales. Tano esteva las vantes e de controles respectivas do dentados a garantiar una correct detección y pesitín de brechas de datos personales.
Procedimiento de ges Pracada factor de riesgo, es nece las los lajuientes pasos: los latados de meditas que se pue difontando las peculiaridades conc Paso 1 Paso 2	tión para reducir el riesgo serio seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son exhaustivo; ni obligatorios, ni de medidos minimos, sino ilustrativos. El responsable o encorgodo han de gestionar el riesgo ten de la nataminimo Medidas de mitigación asociadas a determinados factores de riesgo Medidas de mitigación asociadas a determinados factores de riesgo Necessaria el se de la nataminimo de la desego de la desego respo Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas físicas Han de establecente controles reguelloso rientados a garantiar una correcta detección y gestión de brechas de dictos personales na el DEX, ampliando a medidas para garantiar la resiliencia, azí como para prevenir los falos y errores en las garantias de sinteriorie. Monter medidar
Procedimiento de ges Procedimiento de rieso, es neci- rias los liguientes pasos: los listedes de melhas que se pue generato la preculiaridades conc Paso 1 Paso 2 Paso 3	tión para reducir el riesgo taxio seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar mo son enhaustion, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo den seleccionar no son enhaustion, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo Medidas de mitigación asociadas a determinados factores de riesgo Begin el fector de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de riesgo. Locara medida: Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas físicas Han de stubilecem contines regalificas oxietandos a garentirar una correcta detección y petión de brechas de datos personales. Regione medida: Para proteger la seguridad de los datos para los derechos y libertades de las personas físicas Han el tótis, majendas en endias para guesantar la resiliencia, al como para prevenir los fallos y errores en las gaentas de protección de datos y aplicaciones. Locara medida: Medidas de mitigación organizativas, de gobernanza y políticas de protección de datos Medidas generales y comunes para tados los factores de riesgo. En función del niel de riesgo de tratamiento se habeis de ser más ingente con estas medida.
Procedimiento de ges Pras cada factor de riesgo, es nece rias a cada factor de riesgo, es nece la clatada de meditas que se pue diportando las peculiaridades conc Peso 1 Peso 2 Paso 3	tión para reducir el riesgo texito seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son enhanstino, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo den seleccionar no son enhanstino, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo Medidas de mitigación asociadas a determinados factores de riesgo Begin el fector de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de riesgo.
Procedimiento de ges Pracada factor de riesgo, es nece las cada factor de riesgo, es nece las los de guiernes pasos: a los ladas de mediais que se pue difontendo las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces	tión para reducir el riesgo tesro seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son enhanstino in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo test a su unatumanto Medidas de mitigación asociadas a determinados factores de riesgo Medidas de mitigación asociadas a determinados factores de riesgo Regin el fector de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de riesgo.
Procedimiento de ges Pracedintento de riesgo, es nece las cada factor de riesgo, es nece las los de juvientes pasoa: la lastada de meditas que se pue difontando las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces 8 Articula 57.b del ROPD en nel aconcertor	tión para reducir el riesgo tesro seleccionar medidas que podrían adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció den seleccionar no son exhaustiva, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo den seleccionar no son exhaustiva, in obligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo Medidas de mitigación asociadas a determinados factores de riesgo Begin el fector de riesgo seleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de riesgo. Locara medida: Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertados de las personas físicas Han el tolis, migiados medidas para grantitar una cometa detección y pesión de brechas de datos personales. Ana poleger la seguridad de los datos para los derechos y libertados de las personas físicas Locara medida: Para proteger la seguridad de los factores a los derechos y libertados de datos y aplicaciones. Locara medida: Medidas de mitigación organizativas, de gobernanza y políticas de protección de datos Medidas de mitigación organizativas, de gobernanza y políticas de protección de datos Medidas de mitigación organizativas, de gobernanza y políticas de protección de datos mignet con estas medidas. Locara medida
Procedimiento de ges las cada factor de riesgo, es nece iga los tiguientes pasos: la latolado de meditar que se pue feontando las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la necces 3 Artículo 35.7b del RGPD en rela adace en resizar una pondenoi	tickano praz reducir el riesgo tistano solateccionar medidas que podrion adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para syudar a su selecció de ristacionar no son enhantínes, ni obligatorios, ni de medidas minimas, sino illustrativos. El responsable o encargado hon de gestionar el riesgo retas de su tratamiento Medidas de mitigación asociadas a determinados factores de riesgo. Según el factor de riesgo aeleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de les detas para los derechos y libertades de los datos para los derechos y libertades de las presonas fisicas. Medidas de ogestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las presonas fisicas. Medidas de positión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fisicas. Medidas de positión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fisicas. Medidas de netificación especificacionientados a garantícar una conceta detección y gestión de brechas de datos personales. Medidas de detios y aplicaciones. Medidas de mitigación organizativas, que tomorea la funcione nata detección y gestión de brechas de datos personales. Medidas generales y comunes para todos los factores de riesgo. En función del niel de riesgo del tratamiento se habrid de ser más segures contecidas a para todos los factores de riesgo. En función del intel de riesgo del tratamientos a habrid de ser más segures contecidas a texa ciencidas. Medidas generales y comunes para todos los factores de riesgo. En función del niel de riesgo del tratamientos a habrid de ser más segures contecidas a texa ciencidas. Medidas personales de texa medidas. Medidas personales de texa medidas. Medidas de terratamiento e la necesidad y la proporcionalidad de las operaciones del
Procedimiento de ges ina cada factor de riesgo, es nece iga los tiguientes pasos: la lostados de meditas que se pue feontando las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces sub adactor en realizar una pondenci letter Rellemen las compos a contin Valudo de Idoneladal Instruccione	tión para reducir el riesgo tión para reducir el riesgo tion valencionar medidas que podrion adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para syudar a su selecció den seleccionar medidas que podrion adoptarse para gestionar el riesgo teres de su otaminaria de su otaminaria de su otaminaria en adolgatorias, ni de medidas minimas, sino ilustrativos. El responsable o encargado hon de gestionar el riesgo Recidas de mitigación asociadas a determinados factores de riesgo Según el factor de riesgo seleccionado se muestran algunas medidas de miligación, que pueden ser comunes a otros factores de riesgo. Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas físicas Man de stabiescen contoles especificas orientados a garantizar una correcta detección y gestión de brechas de datos personales. Recitar medida protección de datos y para los derechos y libertades de las operandes las de atos personales. Recitar medida Medidas de ontilización comandos a garantizar una correcta detección y gestión de brechas de datos personales.
Procedimiento de ges Pracediniento de ges Praceda factor de riesgo, es nece riga los iguientes pacos: as latabas de mediatis que se pue fontendo las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces Evaluación de la neces Evaluación de la neces Evaluación de la neces Evaluación de la neces	tión para reducir el riesgo serio seleccionar medidas que podrin adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selección der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, a nel debigatorios, que pueden ser comunes a otros factores de riesgo.
Procedimiento de ges Pracediniento de ges Praceda factor de riesgo, es nece riesgo los siguientes pasos: los latados de mediatis que se pue ferontendo las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la necces E Artículo 32-26 del ROP en rela el Artículo 32-26 del ROP en rela en actuer en realizar una ponderación tuicio de idoneidad Instrucciones	tión para reducir el riesgo texis seleccionar medidas que podrian adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, indeligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enhoustion, a nel debigatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo Medidas de entitigación asociadas a determinados factores de riesgo Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fisicas Muestades de las personas fisicas Muestades de medias para garantiar una corneta detección y gestión de brechas de datos personales. Response y seguridad de los datos para los derechos y libertades de las personas fisicas, se recomienda el criterio establecido protección de datos y aplicaciones. Recentemende Medidas generales y conunes para todos los factores de riesgo. En función del niel de riesgo del tratamiento se habrid de ser mis segurar con estas medidas. Recentemende indecidas personas field el tratamiento (EIPD) dión con el EDP requiere una evaluación de la necescida y la proporcionalidad de las operaciones del tratamiento, que seguin las guías del EDPS se nateradero a tars contexis:
Procedimiento de ges has cada factor de riesgo, es nece iças los âguientes pasos: los taldatos de meditas que se pue difontando las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces D Articulo 37.3 pel ROP on rela raduce en realizar una ponderació tude necesidad Instruccione	tión para reducir el riesgo texis seleccionar medidas que podrin adoptarse para gestionar el riesgo para los derechos y libetades de los interesados. Para ayudar a su seleccio der seleccionar no son enbaustion, indoligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enbaustion, indoligatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar no son enbaustion, a lodigatorios, ni de medidas minimas, sino ilustrativos. El responsable o encargado han de gestionar el riesgo der seleccionar os son enbaustion a dogutar a su sentidas de miligación, que pueden ser comunes a otros factores de riesgo.
Procedimiento de ges Pracada factor de riesgo, es nece aja los águientes pasos: los taladas de meditas que se pue difontando las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces B Artículo 337.b del RGPD en rela adades en resiltar una pondensi B Artículo 337.b del RGPD en rela adades en resiltar una pondensi tucio de ideneidad (nuturciones	bidding para reducir el riesgo bidding para reducir el riesgo para los derechos y libertades de los interesados. Para syndar a su selecció de instanciano no son enhantine, ni obligatorios, ni de medidas minimas, sino illustrativos. El responsable o encargado hon de gestioner el riesgo el es otranomiento: Medidas de mitigación asociadas a determinados factores de infigación, que pueden ser comunes a otros factores de inego. Cuettor medida: Según el factor de riesgo asleccionado se muestran algunas medidas de mitigación, que pueden ser comunes a otros factores de inego. Cuettor medida: Medidas de positión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fricas. Medidas de positión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fricas. Weidas de positión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fricas. Medidas de las personas fricas. Weidas de cating y aplicaciones. Cuettor medida: Nenteres para los derechos y libertades de las personas filos. Medidas de personas fricas. Cuettor medida: Nenteres para los derechos y libertades de las paralitas de las personas filos. Medidas de personas fricas. Cuettor medida: Nenteres para los derechos de intego. Medidas de personas fricas. Cuettor medida: Cuettor medida: Medidas gonerales y comunes para todos los factores de inego. En funcción de da los y encores ne integrica
Procedimiento de ges Pracediniento de ges Pracediniento de riesgo, es nece riesgo los iguientes pasos: los latados de medicia que se pue feortendo las peculiaridades conc Paso 1 Paso 2 Paso 3 Evaluación de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula de la neces 1 Artícula 527.b del ROP on reju regular de la neces 1 Artícula 527.b del ROP on reju 1 Artícula de la neces 1 Artícula 527.b del ROP on reju 1 Artícula 627.b del neces 1 Artícula 627.b del a neces 1 Artícula 527.b del neces 1 Artícula 527.b del ROP on reju 1 Artícula de la neces 1 Artícula 527.b del neces 1 Artícula 7.b del neces 1 Artícula 527.b del neces 1 Artícula 627.b del neces 1 Artícula 527.b del neces 1 Artícula 627.b del neces 1 A	tión para reducir el riesgo texaio seleccionar medidas que podrina adoptarse para gestionar el riesgo para los derechos y libertades de los interesados. Para ayudar a su selecció der seleccionar no son enboustica, ni adoigatorios, ni de medidas mininas, sino ilustrativos. El responsable o encargodo han de gestionar el riesgo der seleccionar no son enboustica, ni adoigatorios, ni de medidas mininas, sino ilustrativos. El responsable o encargodo han de gestionar el riesgo der seleccionar no son enboustica, no debigatorios, ni de medidas mininas, sino ilustrativos. El responsable o encargodo han de gestionar el riesgo der seleccionar para de senestran algunas medidas de miligación, que pueden ser comunes a otros factores de regen. Locare medida Medidas de gestión de brechas de datos personales y seguridad de los datos para los derechos y libertades de las personas fisicas. Ma de stabilecte montoles especificas orientados a garantiar run a contest detección y gestión de brechas de datos personales. Locare medida protección de datos y aplicaciones. Locare medida Medidas geneticas y comunes para toso de tectos de riesgo. En función del niel de riesgo del tratamiento se habrid de ser em sogente con estas medidas as garantizar tratalismos, factores de riesgo. Ma función del niel de riesgo del tratamiento se habrid de ser met sogente con estas medidas. Locare medida de las operaciones del tratamiento se habrid de ser met sogente con estas medidas. Locare medida Locare medida Locare medida



La valoración del riesgo muestra los resultados del cálculo del riesgo intrínseco del tratamiento, según los factores de riesgo seleccionados, y el riesgo residual, según las medidas de mitigación seleccionadas. Si se cumple una de las condiciones de obligatoriedad para realizar un EIPD se indica, así como la recomendación de EIPD si el riesgo es alto.

Valoración Riesgo Intrínseco	Valoración Riesgo Residual
(0.875) Riesgo Alto	(0.772) Riesgo Medio
SE RECOMIENDA EIPD	
Figura 24 Riesgo	alto, EIPD recomendado



Figura 25 Se cumple alguna condición de EIPD obligatorio

La tabla resumen muestra los factores de riesgo identificados por categorías (la categoría se muestra con un fondo de color distinto según se hayan aplicado medidas de mitigación o no) junto con las medidas proporcionadas o las adicionales que se han introducido para un factor de riesgo de esa categoría.

Las medidas alternativas que se han seleccionado, es decir aquellas que la herramienta no asigna de manera predeterminada a un factor de riesgo, pero el responsable ha seleccionado, se muestran al final de la tabla, junto con las medidas organizativas y de gobernanza comunes.

La siguiente figura muestra un ejemplo (aleatorio) en donde se aprecia lo descrito:



Gestiona	a RGPD				-;¢	(- Castella	ano English	?
[Nombre y datos de contacto d	lel Responsable] - Tro	atamiento 2: Tra	tamiento 2				🐴 Inicio	
Finalidades Tipos Extensión In	teresados Técnicas Re	ecogida Efectos	Responsables	Comunicaciones	Otros	Seguridad	Gestión del Ries <u>c</u>	90

Gestión del riesgo del tratamiento : Tratamiento 2

09/04/2024

aloración Riesgo Intrínseco	Valoración Riesgo Residual				
🕽 (0.779) Riesgo Medio	(0.500) Riesgo Medio				
uentes de riesgo identificadas (a	igrupadas por categorías):				
Finalidades	No se han especificado factores de riesgo				
Tipos	No se han especificado factores de riesgo				
Extensión	Sistemático - Mitigación: Limitadamente mitigado				
	Medidas de mitigación/control				
	 Aislar y segregar fases del tratamiento entre sí para que traten datos de una forma más limitada. Por ejemplo haciendo que algunas fases no traten datos personales (p.ej. datos anonimizados) o recurriendo a su seudonimización. 				
- Definir dentro del tratamiento casos de uso concretos con ámbitos disjuntos.					
	- Eliminar alguna fase del tratamiento.				
	- Limitar en la concepción del tratamiento el tiempo en el que el tratamiento trata datos de los mismos sujetos.				
Interesados	Personas mayores - Mitigación: No mitigado				
	Medidas de mitigación/control				
Técnicas	No se han especificado factores de riesgo				
Recogida	No se han especificado factores de riesgo				
Efectos	No se han especificado factores de riesgo				
Responsables	No se han especificado factores de riesgo				
Comunicaciones	No se han especificado factores de riesgo				
Otros	No se han especificado factores de riesgo				
Seguridad	No se han especificado factores de riesgo				
	Medidas de mitigación/control				
	- (ENS op.pl.4) Planificación: Dimensionamiento/gestión de la capacidad				
	- Procedimientos de notificación a la Autoridad de Control para poder cumplir con los requisitos del artículo 33.				

Otras medidas de mitigación/control seleccionadas para los factores de riesgo

- Utilizar técnicas avanzadas de cifrado en reposo y desde el responsable (ZKP, homomórfico,...)

Medidas de mitigación organizativas, de gobernanza y políticas de protección de datos

- Políticas en los procedimientos: Están incluidos en los procedimientos de adquisición de productos, sistemas o servicios que van a implementar operaciones dentro de la actividad de tratamiento el requerir información y garantías para asegurar y poder demostrar que dicho tratamiento cumple con el RGPD.

Figura 26 Tabla resumen

La evaluación de necesidad y proporcionalidad de las operaciones de tratamiento (EIPD) proporcionan ayuda para rellenar los campos disponibles, posicionando el ratón sobre los textos subrayados y el icono con la letra 'i' de información. No obstante, hay que tener en



cuenta que el uso de esta herramienta no supone dar por realizada de forma automática la EIPD.

🚍 🔂: Gestiona RGPD	ː Castellano English (?)
Finalidades Tipos Extensión Interesados Técnicas Recogida Efectos Responsables Comunicaciones Otros Seguridad Gestión do	el Riesgo
Evaluación de la necesidad y proporcionalidad del tratamiento (EIPD)	
El Artículo 35.7.b del RGPD en relación con el EIPD requiere una evaluación de la necesidad y la proporcionalidad de las operaciones del tratam traduce en realizar una ponderación atendiendo a tres criterios:	niento, que según las guías del EDPS se
Nota: Rellenar los campos a continuación, así como el uso de esta herramienta no supone dar por realizada la EIPD	
Juicio de idoneidad Instrucciones para rellenar este campo 👔	
Juicio de Idoneidad	
En el juicio de idoneidad se debe evaluar si la propuesta de tratamiento, tal y como está planteada, alcanza la eficacia necesaria para cum eficacia, necesariamente, deberá ser demostrada de forma objetiva por el responsable del tratamiento, para lo cual hay que realizar la:	plir los fines que persigue. Esa
 Definición del umbral de efectividad del tratamiento: Establecer de forma objetiva, cualitativa y basada en evidencias, cuál es el umbra alcanzar para cumplir con los fines del tratamiento (algunos ejemplos podrían ser, un margen de error del 5% en un valor resultado, u una posibilidad de fraude por debajo del 1%). Evaluación de la efectividad de la propuesta de tratamiento: Evaluar de forma objetiva, cualitativa y basada en evidencias, la efectivida planteado, verificando si da respuesta a las necesidades planteadas y con qué extensión (determinar si genuinamente resuelve dichas 	al de efectividad que se debería una detección de un 95% de casos o ad del tratamiento, tal y como se ha s carencias).
La evaluación de la idoneidad ha de ser racional, analítica y basada en hechos y datos objetivos. Hay que aceptar la realidad de que en cua cualquier tratamiento es imposible alcanzar la perfección. Aparte de que no es eficiente desde el punto de vista económico, ni viable técni que impiden la eficacia total, especialmente en temas de seguridad. Asumiendo dicha realidad, hay que determinar el nivel aceptable de e estricta necesidad y demostrar que el tratamiento propuesto lo alcanza.	alquier tipo de finalidad y para icamente, existen múltiples factores fficacia requerido para cumplir con la
En base a la información obtenida en este análisis, se decidirá seguir o no adelante con el tratamiento tal y como está planteado.	
B <i>I</i> ⊻ Ξ :Ξ	
Juicio de necesidad Instrucciones para rellenar este campo 🕧	
$\mathbf{B} \mid \mathbf{I} \mid \mathbf{U} \mid \mathbf{\Xi} \mid \mathbf{\Xi}$	

Figura 27 Ayuda para rellenar el Juicio de Idoneidad

Una vez terminada la evaluación de riesgos de un tratamiento, se ha de regresar a la pantalla de inicio (gestión de tratamientos) donde se podrán generar informes y guardar los tratamientos en un archivo.

D. FINALIZAR LA SESIÓN, GUARDAR DATOS Y SALIR DE LA APLICACIÓN

Una vez que se ha terminado con la introducción o edición de tratamientos y la evaluación de riesgos correspondientes es necesario guardar los datos, pues al cerrar la pestaña del navegador o actualizarla los datos, que están en la memoria local del navegador en la sesión que se tiene abierta se perderán. La página avisa mediante un mensaje del navegador.

Para guardar los datos ha de usarse el botón *Guardar* de la página de Inicio. Es importante recordar que se guarda un archivo con un nombre predefinido, siempre el mismo: *Tratamientos_de_datos.aepd* (que el usuario podrá renombrar una vez guardado). Dependerá de las opciones de configuración del navegador si se guarda directamente en la carpeta de descargas del ordenador, en alguna carpeta temporal o se abre un explorador de archivos para elegir dónde.



No se modifican o actualizan archivos previamente cargados, el usuario habrá de llevar un control de cuál es su último archivo de trabajo.

Registro de Tratamientos y Evaluación del Riesg	¿Quieres salir del sitio web? Es posible que los cambios no se guarden. Salir Cancelar	☆: Castellano English ? ardar ⚠ Cargar 🖨 Informes / Exportar •
Responsable del Tratamiento	0	
[Nombre y datos de contacto del Responsable [Dirección completa] [teléfono] [email] [Descripción breve de la actividad desarrollada] ejercicio de derechos: [email_ejercicio_derechos. [Datos del delegado de protección de datos]] [NIF]]	
(Para cambiar estos datos y el DPD edite y modifiqu	e el primer tratamiento de la lista)	
Tratamientos de datos perso A continuación se relacionan los distintos tipos de	nales tratamientos de datos personales:	

	Expandir todos
Tratamiento 1	~
Tratamiento 2	~

Figura 28 Aviso al cerrar la pestaña del navegador

III. REFERENCIAS

- Herramienta GESTIONA RGPD para la gestión del RAT, generación de inventario, evaluación y gestión del riesgo para los derechos y libertades [jun 2023]
- <u>Gestión del riesgo y evaluación de impacto en tratamientos de datos personales</u> [jun 2021]
- Sitio web de la División de Innovación Tecnológica de la AEPD