Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Marc Rodríguez Ferrer

Tutor: Juan Vicente Oltra Gutiérrez

2019-2020

Resumen

Desde la década de los cincuenta, se han ido desarrollando mecanismos legales con el objetivo de proteger a la sociedad en el ámbito de la privacidad y de sus datos personales. Con la puesta en funcionamiento del Reglamento General de Protección de Datos a mediados del 2018, toda Europa adoptó un mismo marco normativo de aplicación inmediata con el objetivo de facilitar una puesta en marcha común en sus estados miembros. ¿Es tan sencillo como parece?

En este trabajo explicamos las novedades que trae este nuevo reglamento y los cambios que conlleva para los profesionales de la protección de datos. Mostramos una hoja de ruta a seguir para garantizar el correcto cumplimiento normativo dentro de cualquier organización, siendo capaces de adoptar un papel proactivo para anticiparse a las posibles amenazas sobre los derechos y libertades de los usuarios. Con la hoja de ruta pueden aprender a realizar análisis de riesgos y evaluaciones de impacto que permiten trazar un plan para aplacar los posibles riesgos generados a la hora de tratar datos personales.

Realizamos un balance de estos dos últimos años, desde su entrada en funcionamiento, y nos hacemos eco de algunas noticias de actualidad que han aparecido en los medios. Estas están relacionadas con una gestión inadecuada de algunas directrices que nos proporciona la normativa.

Concluimos el proyecto plantando la semilla de una aplicación que será desarrollada en un futuro proyecto y que se puede utilizar como plantilla para construir una herramienta de apoyo para los responsables de protección de datos.

Palabras clave: amenaza, riesgo, evaluación, impacto, reglamento, protección, datos, RGPD

Resum

Des de la dècada dels anys cinquanta, s'han anat desenvolupant mecanismes legals per a tractar de protegir a la societat en l'àmbit de la privacitat i de les seues dades personals. Amb la posada en funcionament del Reglament General de Protecció de Dades a mitjans del 2018, tota Europa va adoptar un mateix marc normatiu d'aplicació immediata amb l'objectiu de facilitar una implantació comú en tots els seus estats membres. Serà tant senzill com pareix?

En aquest treball expliquem les novetats que inclou el nou reglament i els canvis que comporta per als professionals de la protecció de dades. Mostrem un full de ruta a seguir per a poder garantir el correcte compliment normatiu dins de qualsevol organització, sent capaços d'adoptar un paper proactiu per a poder avançar-nos a les possibles amenaces sobre els drets i llibertats dels usuaris. Amb el full de ruta poden aprendre a realitzar anàlisis de riscs i avaluacions d'impacte que permeten tindre un pla per a mitigar els possibles riscs generats a l'hora de tractar dades personals.

Revisem la situació d'aquets darrers dos anys, des de la seua entrada en funcionament, i analitzem algunes noticies d'actualitat que han aparegut als mitjans de comunicació. Aquestes estan relacionades amb una gestió inadequada d'algunes directrius que ens proporciona la normativa.

Per acabar, plantegem les bases d'una aplicació que serà desenvolupada en un futur projecte i que es pot fer servir com una plantilla per a construir una ferramenta en la que es recolzaran els responsables de la protecció de dades.

Paraules clau: amenaça, risc, avaluació, impacte, reglament, protecció, dades, RGPD

Abstract

Since the 1950s, legal mechanisms have been developed aiming to protect society in terms of privacy and personal data. With the implementation of the General Data Protection Regulation by mid-2018, whole Europe embraced the same legal framework with the goal of facilitating an implementation of a common strategy in its member states. Is it as simple as it looks?

In this document, we explain the new developments that this recent regulation brings, and related changes that it entails for data protection professionals. We show a roadmap to follow in order to ensure correct regulatory compliance in any organization. Thus, they will be able to take a proactive role by anticipating potential threats about the rights and freedoms of users, which may occur. With the roadmap they can learn how to perform risk analyses and impact assessments that allow drawing up a plan to appease potential risks generated when processing personal data.

We review the situation over the last two years, since its implementation, and we analyse the latest news. These are related to an inadequate management of some guidelines provided by the regulation.

We conclude the project by planting the seed of an application that will be developed in a future project, and which can be used as a template to build a tool for data protection managers.

Keywords: threat, risk, privacy, impact, assessment, data, protection, regulation, GDPR

Lista de figuras

Figura 1: Digital around the world in 2020 (Kemp 2020) 11
Figura 2: Leyes de Protección de Datos en España (Elaboración propia) 23
Figura 3: Etapas de la gestión de riesgos (Elaboración propia) 34
Figura 4: Fases del ciclo de vida de una actividad de tratamiento de datos (Elaboración propia) 42
Figura 5: Elementos en cada etapa del ciclo de vida de los datos (Elaboración propia) 43
Figura 6: Fases a seguir en la Evaluación de Impacto de Protección de Datos (Elaboración propia) 46
Figura 7: Definición de riesgo en función del impacto y la probabilidad (Elaboración propia) 51
Figura 8: Herramientas AEPD para cumplimiento normativo (Elaboración propia) ... 56
Figura 9: Fases para el planteamiento de la herramienta propuesta (Elaboración propia) 62
Figura 10: Boceto de la ventana inicial de la herramienta (Elaboración propia) 64
Figura 11: Boceto de la ventana del panel de herramientas (Elaboración propia) 65
Figura 12: Boceto de la ventana principal de la herramienta seleccionada (Elaboración propia) 66
Figura 13: Boceto de la ventana del formulario de datos de las herramientas (Elaboración propia) 67
Figura 14: Duración de las fases del proyecto (Elaboración propia)..... 68
Figura 15: Arquitectura de 3 capas (Elaboración propia) 70
Figura 16: Diagrama de casos de uso de la herramienta (Elaboración propia) 72
Figura 17: Logo de la aplicación Mitiga2 (Elaboración propia) 73
Figura 18: Ventana de inicio de sesión de la aplicación (Elaboración propia) 74
Figura 19: Ventana del panel de herramientas de la aplicación (Elaboración propia)...75
Figura 20: Ventana principal de las herramientas RAT, ABR y EIPD (Elaboración propia) 76
Figura 21: Ventana de recogida de datos de las herramientas RAT, ABR y EIPD (Elaboración propia) 76

Lista de tablas

Tabla 1: Modelo de dos capas en la política de privacidad (Elaboración propia) 31

Tabla 2: Recogida de datos para identificación de posibles amenazas (Elaboración propia) 44

Tabla 3: Identificación de riesgos y posibles medidas de control (Elaboración propia) 45

Tabla 4: Roles desempeñados por los actores que pueden participar en la EIPD (Elaboración propia) 47

Tabla 5: Matriz de riesgos (Elaboración propia) 52

Tabla de contenidos

1. Introducción 11
1.1 Motivación 13
1.2 Objetivos 14
1.3 Estructura 15
1.4 Convenciones 16
1.5 Limitaciones 16
2. Situación actual 18
2.1 ¿Qué son los datos de carácter personal? 18
2.2 Antecedentes normativos 19
2.3 Implicaciones del RGPD 24
2.3.1 Derechos de los interesados 24
2.3.2 Deberes de las organizaciones 26
2.4 Análisis básico de riesgos 41
2.5 Evaluación de impacto de protección de datos 45
2.5.1 Fases de la EIPD 46
2.5.2 Actores principales en la EIPD 47
2.5.3 Realización de la EIPD 48
2.6 Herramientas de las autoridades de control 54
2.6.1 AEPD 55
2.6.2 APDCat 57
2.6.3 CNIL 58
2.7 Crítica a la situación actual 58
2.8 Balance en estos dos años de funcionamiento 59
2.9 Propuesta de mejora y metodología a seguir 61
3. Análisis de requisitos 63
3.1 Requisitos de seguridad 63
3.2 Boceto de la herramienta 64
3.3 Plan de trabajo seguido del TFG 68
3.4 Presupuesto 69
4. Diseño del sistema 70
4.1 Arquitectura del sistema 70
4.2 Detalle de funcionalidad y casos de uso 71
4.3 Tecnologías utilizadas 73
5. Desarrollo de la interfaz 74

6. Conclusión 78
7. Referencias 80
8. Glosario 84
Anexos 88
I. Plantilla para el registro de actividades de tratamiento 88
II. Formulario para la realización de una EIPD 90

«Lo que no se define, no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre»

(William Thomson, [Lord Kelvin])
1824-1907

1. Introducción

Solo hace falta parar un segundo y mirar a nuestro alrededor… así es, vivimos rodeados de dispositivos cada vez más hiperconectados. La gran cantidad de datos que intercambian entre ellos es prácticamente imposible de procesar por la mente humana. No obstante, parece ser que nuestra confianza en estos pequeños artilugios, día tras día va en aumento. Tal es así que, si nos paramos detenidamente a pensar, no son capaces de funcionar si no los alimentamos confiándoles ciertas dosis de nuestra privacidad. ¿Nos damos cuenta del verdadero poder que tenemos entre manos? Nuestros datos son la moneda virtual más cotizada de la que se nutren todos los nuevos negocios digitales de hoy en día. Los datos son el nuevo petróleo.

Para hacernos una idea de lo conectados que estamos, podemos revisar la siguiente infografía (Caballero Velasco y Cilleros Serrano 2019, p.24) que hemos actualizado con datos de enero del 2020. En ella vemos que, de los más de 7.750 millones de personas que habitamos el planeta, 5.190 millones son usuarios únicos de dispositivos móviles.

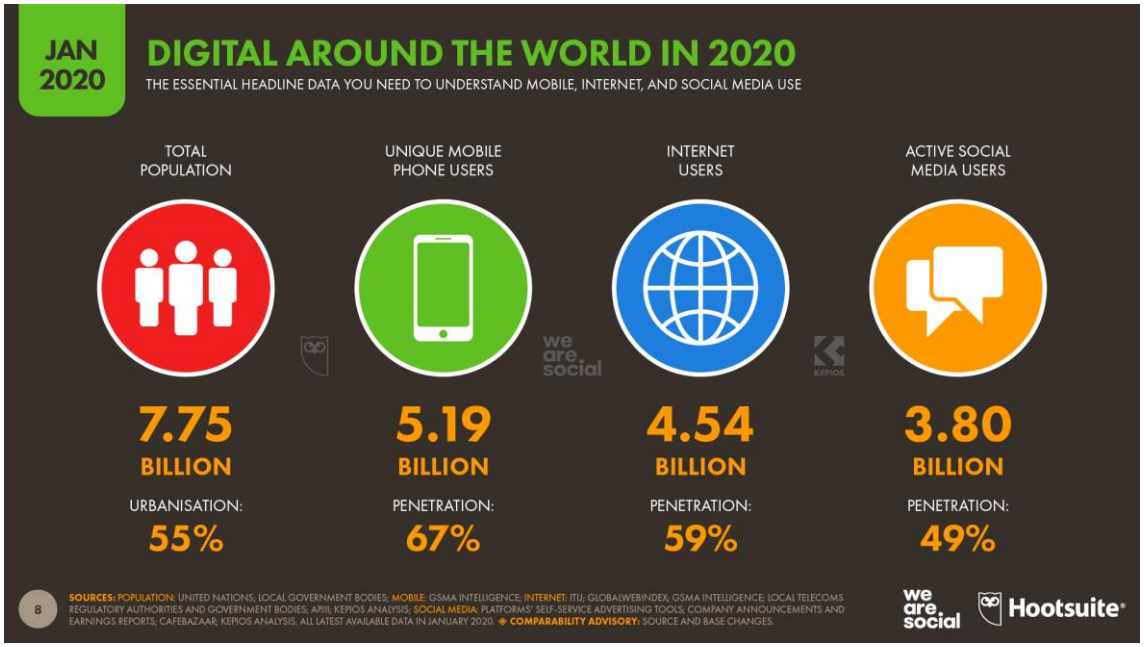

Figura 1: Digital around the world in 2020 (Kemp 2020)

Nosotros, como propietarios de nuestros datos, no debemos descuidar que estos negocios cada vez serán más persuasivos con tal de que les ayudemos a generar valor y a hacer evolucionar sus actuales modelos de negocio. No nos queda otra alternativa que proteger nuestros datos personales [1] para tratar de evitar posibles filtraciones involuntarias.

Las empresas de hoy en día están empezando a tener una cultura del dato más arraigada que años atrás. Gracias al almacenamiento y estructuración de grandes cantidades de datos mediante técnicas de *Big Data*[1] [2] junto con las altas capacidades de procesamiento que nos proporciona la inteligencia artificial [3] y sus ramas *Machine Learning*[2] [4] y *Deep Learning*[3] [5], tratan de encontrar patrones que les ayuden a tomar mejores decisiones y así aumentar su competitividad.

Un ejemplo de ello, son las redes sociales, que como hemos observado en la anterior infografía, casi la mitad de la población tiene cuenta en alguna de ellas. Es por esto por lo que queremos remarcar que la mayoría de estas plataformas son gratuitas debido a que se nutren de la utilización de los datos que les vamos proporcionando. Cada vez que compartimos ubicaciones, noticias, gustos, preferencias… les ayudamos a obtener ingresos, la mayoría son de tipo publicitario. El usuario es el principal elemento que monetizar por parte de la red social. Cuanto mayor número de usuarios activos, mayor valor se le da a la plataforma. A veces los usuarios no somos conscientes que nuestros datos pueden ser accesibles desde cualquier parte del mundo, con los riesgos que esto conlleva. No todos los países tienen la misma legislación en cuanto a los derechos de protección de datos personales y por tanto sus medidas de aplicación pueden no ser lo suficientemente rigurosas para evitar filtraciones de datos.

Hace poco fuimos testigos del escándalo ocurrido con Facebook y Cambridge Analytica (BBC NEWS 2019), donde los datos personales de 87 millones de usuarios fueron explotados sin el consentimiento de los interesados [6], para influir en las pasadas elecciones presidenciales en Estados Unidos.

Debido a toda esta vorágine del dato en la que estamos inmersos, existen regulaciones y leyes que nos amparan y nos marcan unas pautas a seguir para que seamos conocedores de los derechos que tenemos relativos al intercambio de nuestros datos con otros usuarios u organizaciones.

En este proyecto, nos centraremos en las diferentes leyes cuyo objetivo principal ha sido el de proponer medidas de contención y protección sobre los datos de carácter personal. Haremos un breve recorrido por nuestra historia reciente donde resaltaremos los mecanismos legales hemos ido adoptando en España para esta finalidad, hasta llegar al momento de la entrada en vigor del nuevo Reglamento General de Protección de Datos (en adelante RGPD) que es de obligado cumplimiento a nivel europeo, desde

[1] Big Data: «macrodatos» o «inteligencia de datos», (Fundeu 2013).
[2] Machine Learning: «aprendizaje automático», (Linguee 2020).
[3] Deep Learning: «aprendizaje profundo», (Linguee 2020).

el 25 de mayo del 2018. Como consecuencia del nuevo reglamento, en España actualizamos nuestra antigua Ley Orgánica de Protección de Datos adaptándola las nuevas directrices nuevo reglamento europeo. Estas novedades se plasmaron en la nueva Ley Orgánica de Protección de Datos y garantías de los Derechos Digitales (en adelante LOPDGDD).

1.1 Motivación

La elección de este trabajo de fin de grado relacionado con las novedades que conlleva la entrada en vigor del RGPD, se debe a la necesidad de facilitar a las organizaciones, una guía que ayude al responsable [7] de protección de datos para garantizar el correcto cumplimiento normativo. Sin importar el tamaño ni el tipo de empresa ya que el RGPD afecta a todas: desde el pequeño autónomo a las grandes multinacionales.

Tras su entrada en vigor, hace poco más de dos años, sigue generando confusión a la hora de gestionar los tratamientos [8] de datos personales en los procesos internos de la empresa. Por ello nos hemos propuesto aportar claridad sobre las nuevas obligaciones que se presentan, ya que suele ser un tema que no recibe la importancia que merece. Debemos asumir que ignorar la ley no exime de su cumplimiento.

Como veremos, una pequeña filtración de datos personales en cualquier organización puede convertirse en un problema con graves consecuencias económicas, además de causar pérdidas de confianza y competitividad. Muchas de las *startups*[4] [9] de nueva creación, al estar relacionadas con las nuevas tecnologías, además de los riesgos relacionados con la protección de datos, también tienen riesgos inherentes a la ciberseguridad.

En la época de transformación digital en la que nos encontramos, es importante conocer al detalle la normativa para saber cómo poder trabajar con esos datos personales de manera correcta. Esto es un pilar fundamental necesario para los profesionales del sector que nos dedicamos a mejorar los flujos de trabajo en las empresas mediante la inclusión de nuevas tecnologías en ciertos procesos que no aportan valor al trabajo realizado por los compañeros en los diferentes departamentos.

Un ejemplo de ello podría ser la progresiva digitalización de los procesos que conllevan intercambio de información mediante documentación en formato físico, ya que una mala praxis en la gestión del papel, lo podemos considerar como una amenaza [10]

[4] Startup: «Empresa emergente».

que puede acarrear un riesgo [11]. El uso de herramientas software como gestores documentales, nos permiten minimizar riesgos humanos y nos aportan ventajas a la hora de compartir información entre nuestros compañeros, algo tremendamente útil en la situación vivida durante estos últimos meses con la obligación de priorizar el teletrabajo debido a la emergencia sanitaria por la COVID-19.

Fuera del ámbito laboral, como usuarios de muchos servicios, con esta guía podremos conocer con más detalle nuestros derechos a la hora de ceder nuestros datos personales.

1.2 Objetivos

Como hemos introducido en el apartado anterior, el principal objetivo del trabajo es que pueda ser utilizado como guía para que los responsables de protección de datos de las organizaciones puedan garantizar el cumplimiento normativo. En este documento se recogerán las directrices que el profesional deberá seguir para conocer cómo llevar a cabo una evaluación de impacto en caso de ser necesaria, ya que es una de las novedades que incluye el RGPD.

Para ello, analizaremos el contenido jurídico del nuevo reglamento y nos apoyaremos en las guías o herramientas que nos proporcionan diferentes autoridades de control [12], como la Agencia Española de Protección de Datos (en adelante AEPD), la Autoridad Catalana de Protección de Datos (en adelante APDCat), la Agencia Vasca de Protección de Datos (en adelante AVPD) y por último o la autoridad francesa *Commission Nationale de l'Informatique et des Libertés*[5] (en adelante CNIL).

¿Por qué tres españolas y una francesa? Aunque el RGPD es el mismo en toda Europa, cada autoridad de control tiene la libertad de crear guías y herramientas que ayuden a los ciudadanos a entender y aplicar correctamente la normativa. En España hoy en día tenemos tres. Queremos aclarar que la APDCat y la AVPD, gestionan los datos personales de las administraciones en sus respectivas comunidades autónomas junto con la supervisión de la AEPD. La AEPD, como entidad a nivel estatal, gestiona todos los datos relacionados con las empresas, y de las demás administraciones autonómicas que no tienen una autoridad de control dedicada. Hemos elegido también la CNIL porqué nos ha llamado la atención la herramienta que han creado para llevar a cabo las evaluaciones de impacto. Posteriormente hablaremos de ella.

[5] Commission Nationale de l'Informatique et des Libertés: «comisión nacional de informática y libertades» (Linguee 2020).

La comparativa sobre las guías y herramientas de las autoridades de control elegidas, nos ayudará a obtener una metodología para poder llevar a cabo una evaluación de impacto correctamente, además de demostrar cumplimiento normativo.

Con todo el conocimiento adquirido, y tras haber finalizado la guía, propondremos el desarrollo de una herramienta software en la que podremos plasmar la metodología aprendida, y que podrá ser usada para facilitar la labor de los profesionales de la protección de datos. Para ello, analizaremos los requisitos que consideremos necesarios y diseñaremos un boceto. Posteriormente explicaremos el comportamiento propuesto y diseñaremos la interfaz de la herramienta cuyo completo desarrollo, implantación y fase de prueba, se llevarán a cabo en un futuro proyecto.

1.3 Estructura

Después de realizar una pequeña introducción y plantear los objetivos que vamos a perseguir durante el desarrollo del trabajo, vamos a explicar el contenido que nos encontraremos en los próximos capítulos del presente documento.

En el capítulo 2, nos pondremos en contexto al revisar los antecedentes del RGPD. Explicaremos todas las novedades que conlleva su aplicación junto con los derechos de los usuarios y obligaciones de las organizaciones. Propondremos unas pautas a seguir para demostrar cumplimiento normativo en las empresas y desarrollaremos la metodología a seguir para llevar a cabo un análisis de riesgos y una evaluación de impacto. Para acabar el capítulo, repasaremos las herramientas gratuitas que ofrecen algunas autoridades de control y repasaremos como le ha ido al RGPD en estos dos años desde su entrada en vigor.

En el capítulo 3, con toda la metodología aprendida, propondremos el desarrollo de una aplicación que será el germen de otro proyecto continuista. Analizaremos las necesidades que nos permitan llevarla a cabo y propondremos un boceto. También indicaremos la duración de la realización del proyecto y su coste estimado.

En el cuarto capítulo, propondremos sobre qué arquitectura de desarrollo sería conveniente basarse para que los que implementen la herramienta en un futuro, puedan llevarla a cabo. Veremos el funcionamiento básico a través de sus casos de uso y repasaremos las tecnologías que hemos utilizado.

En el quinto capítulo, mostraremos las interfaces creadas y explicaremos su funcionamiento.

En el capítulo 6, sacaremos conclusiones sobre el cumplimiento de los objetivos del proyecto y de las propuestas realizadas.

Para finalizar, hemos añadido un glosario donde explicaremos los términos que aparecen remarcados en esta obra.

1.4 Convenciones

Debido a que durante el desarrollo de la presente memoria se utilizará un lenguaje jurídico para mencionar algunas leyes, directivas, decretos o reglamentos en el ámbito de la protección de datos, nos gustaría indicar que se incluirán literalmente aquellos artículos que consideremos remarcar. Estos irán formateados en cursiva y siempre enmarcados entre «».

También aparecerán entre «» las frases que parafraseemos de personas a las que hagamos referencia y que aparezcan en algún artículo al que hagamos mención, así como las definiciones de los términos del glosario. En este caso no irán en cursiva.

Las palabras o frases extranjeras sobre las que aclararemos su significado a pie de página se mostrarán en cursiva, siempre y cuando no hagan referencia a un nombre propio escrito en otro idioma.

Como hemos añadido un glosario de términos al final del presente documento, durante la lectura de la memoria encontraremos algunas palabras acompañadas de una marca referencial [x], siendo x una referencia al orden de aparición. En el glosario se podrán encontrar los términos ordenados alfabéticamente junto con la referencia comentada.

Las referencias bibliográficas aparecerán ordenadas alfabéticamente.

1.5 Limitaciones

A la hora de añadir las referencias bibliográficas al trabajo, hemos aprendido a utilizar Mendeley, que es una herramienta software que nos ayuda a gestionar la bibliografía que vamos utilizando durante la fase de investigación. Para ello hemos seguido los videotutoriales que nos facilita la UPV a través de su canal de YouTube y que se encuentran agrupados en la lista de reproducción “Gestión de referencias bibliográficas.

Mendeley[6]". Esta herramienta tiene la ventaja de contar con extensiones que se integran en los navegadores web y en el software procesador de textos Microsoft Word, facilitando la inserción de las referencias en la memoria directamente siguiendo la Normativa ISO 690 requerida.

A medida que hacíamos uso de ella, íbamos teniendo cada vez más problemas para agregar correctamente las referencias al documento. Muchas veces por falta de datos en las mismas, y otras veces por errores con las extensiones del navegador y del procesador de textos. Al tener que ir repasando y corrigiendo cada referencia guardada y darnos cuenta del tiempo que esto suponía, tomamos la decisión de buscar algunas guías recomendadas de otras universidades e insertar las referencias de forma manual.

Las guías que hemos utilizado han sido:

- Universidad de Cantabria. «Cómo citar bibliografía según ISO 690[7]».
- Universidad Carlos III de Madrid. «Guía temática sobre citas bibliográficas UC3M: UNE-ISO 690:2013[8]».
- Universidad Autónoma de Madrid. «Citas y elaboración de bibliografía: el plagio y el uso ético de la información, estilo UNE-ISO 690[9]».
- Biblioteca de la Universidad de Sevilla. «Bibliografía y citas: UNE-ISO 690:2013[10]».

[6] Lista reproducción UPV: https://www.youtube.com/playlist?list=PLDNHzv4W4qUNtiPUZmF9LBhlUBrjn0vTz
[7] Guía Universidad de Cantabria: https://web.unican.es/buc/recursos/guias-y-tutoriales/guia?g=159
[8] Guía Universidad Carlos III: https://uc3m.libguides.com/guias_tematicas/citas_bibliograficas/une-iso-690
[9] Guía Universidad Autónoma de Madrid: https://biblioguias.uam.es/citar/estilo_une
[10] Guía Biblioteca Universidad de Sevilla: https://guiasbus.us.es/bibliografiaycitas/estilouneiso

2. Situación actual

Como hemos comentado en la introducción de la memoria, a raíz de la evolución de las tecnologías de la información en estas últimas décadas, como sociedad, nos hemos visto obligados a desarrollar mecanismos legales para amparar los derechos de las personas a la no violación de la seguridad de sus datos personales [13] y su intimidad. Antes de comentar las directrices jurídicas que hemos venido siguiendo estos años, conviene explicar detalladamente qué es lo que consideramos como dato personal.

2.1 ¿Qué son los datos de carácter personal?

Tal y como nos explica la AEPD en el documento "Guía para el Ciudadano", se considera dato de carácter personal a toda información concerniente a una persona física identificada o identificable. Se considerará persona identificable aquella cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador como por ejemplo un nombre, un número de identificación, datos de localización o un identificador en línea. También a través de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Los datos personales los podemos dividir en dos grandes bloques. Por una parte, tenemos los datos no sensibles y por otra parte los datos sensibles o especiales. Dentro de los datos **no sensibles** podemos situar:

- **Datos identificativos**: nombre, apellidos, domicilio, teléfono, correo electrónico, número nacional de identidad, edad, nacionalidad…
- **Datos relativos a características personales**: estado civil, lugar y fecha de nacimiento, edad, sexo…
- **Datos profesionales**: puesto de trabajo, dirección, correo electrónico, teléfono…
- **Datos financieros**: información fiscal, propiedades, cuentas bancarias, ingresos…
- **Datos académicos**: formación, titulaciones, calificaciones…

Dentro de los datos **sensibles** especialmente protegidos tenemos:

- **Datos ideológicos**.
- **Datos relacionados con la orientación sexual**.

- **Datos relacionados con alguna afiliación sindical**.
- **Datos relativos a la salud [14]**.
- **Datos religiosos**.
- **Datos sobre el origen racial o étnico de una persona**.
- **Datos biométricos [15]**.
- **Datos genéticos [16]**.
- **Datos relativos a condenas e infracciones penales**.

Cabe remarcar, que no se consideran datos de carácter personal los referentes a las personas jurídicas que puedan pertenecer a alguna de las categorías anteriores.

2.2 Antecedentes normativos

Para comenzar a adentrarnos en la evolución relativa a la normativa de protección de datos en las últimas décadas, resaltaremos algunos textos normativos previos y nos fijaremos en algunos artículos que nos muestran relevancia sobre conceptos relacionados.

Vamos a tomar como referencia inicial el artículo 12 de la Declaración Universal de Derechos Humanos (o DUDH), proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su resolución 217 A (III), donde se establece lo siguiente:

«Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.» (art. 12 DUDH).

Al poco tiempo, el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales o más conocido como la Convención Europea de Derechos Humanos (o CEDH), que fue adoptado por el Consejo de Europa el 4 de noviembre de 1950, incluía en su artículo 8:

«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.» (art. 8 CEDH).

En España, con la entrada en vigor de nuestra norma suprema del ordenamiento jurídico, La Constitución española de 1978, también se hace alusión a la privacidad e intimidad en los artículos 18.1 y 18.4:

«Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.» (art. 18.1 CE).

«La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.» (art. 18.4 CE).

En 1981, el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en su artículo 1 establece que:

«El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")» (art. 1 C108).

Unos años más tarde, en España, se aprobó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante LORTAD), con la que se lleva a cabo los puntos recogidos en el artículo 18 de la Constitución Española. Con esta ley, los derechos de privacidad, intimidad y protección de datos están cubiertos y amparados por la ley. No se hace referencia a la protección del tratamiento de datos personales en soporte físico, sólo afecta a datos automatizados.

El 24 de octubre de 1995 y tras un largo trabajo de la Unión Europea durante la década de los 80, se aprobó la Directiva 95/46/CE, relativa a la protección de personas físicas en lo respectivo al tratamiento de datos personales y la libre circulación de estos datos. En ella se regula el procesamiento de datos personales dentro de la Unión Europea (UE), ya que no había una legislación inclusiva para permitir el intercambio de datos entre los países miembros.

El 11 de junio de 1999, y tras siete años de la entrada en vigor de la LORTAD, se promulga en España el Real Decreto 994/1999, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros [17] automatizados que contengan datos de carácter personal. Su objetivo es el de establecer medidas de técnicas necesarias para garantizar la seguridad en estos ficheros.

Unos meses después se promulga en España la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD). Con esta ley se lleva a cabo la transposición de la Directiva 95/46/CE al reglamento interno del estado español. Con ello se consigue un desarrollo de protección de datos más completo y por fin se regula el tratamiento de datos personales en soporte físico. Desde este momento, la LORTAD queda derogada.

Unos años después, y con la finalidad de dotar de coherencia a la transposición de la Directiva europea y de desarrollar ciertos aspectos novedosos de la LOPD, se promulga el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante RDLOPD). Con esto se desarrollan las medidas de seguridad que se aplicarán en los sistemas de información que almacenen datos personales y también los principios de la Ley.

Los siguientes años, tras un fuerte avance tecnológico y con un mundo cada vez más globalizado, en el que el intercambio de datos era cada vez mayor, en la Comisión Europea se dan cuenta que la Directiva 95/46/CE que entró en vigor en 1995, se estaba quedando desfasada, ya que esta estableció los principios básicos sobre protección de datos que tenían que regir en los países miembros de la Unión Europea. Cada estado decidía de manera independiente cómo cumpliría esos objetivos. Por ese motivo se acuerda una propuesta para crear un nuevo reglamento enfocado al intercambio de datos de una forma más homogénea.

El 25 de mayo de 2016, entra en vigor el Reglamento 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 (conocido como Reglamento General de Protección de Datos o RGPD) y por el que se deroga la Directiva 95/46/CE. Su aplicación no fue obligatoria hasta el 25 de mayo de 2018, dos años después. Su principal objetivo es establecer un régimen de protección de datos aplicable a todos los estados de la unión europea de manera directa, sin necesidad de una transposición[11] por parte de los estados miembro para adaptar el reglamento al derecho interno. De esta manera, la normativa será la misma para todos y su aplicación será uniforme.

Como en ese momento, en España, tenemos en vigor la LOPD, nos encontramos con la situación de tener dos figuras jurídicas que nos afectan directamente en el ámbito de la protección de datos. Por ejemplo, el RGPD nos indica que, para el tratamiento de

[11] Un Reglamento no necesita ser adaptado o transpuesto a leyes internas como una Directiva.

nuestros datos personales, el consentimiento ha de ser expreso y afirmativo y la LOPD nos dice que puede ser tácito. En este caso el RGPD es más exigente.

Aunque no haya que transponer el RGPD a nuestras leyes internas, sí que habrá que adaptar la LOPD para intentar evitar conflictos o contradicciones que pueda acarrear la aplicación directa del mismo teniendo nosotros una Ley Orgánica para tal fin. Es por eso por lo que se aprueba la elaboración de una nueva Ley Orgánica de Protección de Datos para complementarla. En 2018 se aprueba la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (conocida como LOPDGDD). En ella se reflejan las nuevas medidas impuestas por el RGPD y otras complementarias que tratan de mejorar nuestra ley anterior adaptándola a la actualidad.

Algunas de estas novedades que incluye la LOPDGDD son:

- **Derecho al testamento digital (art. 3 LOPDGDD)**: tenemos el derecho de elegir a algún familiar como heredero de nuestra huella digital. Estos familiares podrán dirigirse a los responsables del tratamiento de nuestros datos personales para solicitar el acceso a los mismos. Este derecho no está contemplado en el RGPD.
- **Consentimiento de los menores de edad (art. 7 LOPDGDD)**: el RGPD nos indica que la edad mínima para dar consentimiento del tratamiento de los datos personales de un usuario tiene que ser a partir de los trece años. La LOPDGDD establece la edad de catorce años.
- **Derecho a limitar la actividad publicitaria de las empresas (art. 23 LOPDGDD)**: como ciudadanos podemos limitar la publicidad no deseada. Existen plataformas como La Lista Robinson[12] creadas con esa finalidad.
- **Derecho a la neutralidad de internet (art. 80 LOPDGDD)**: no se puede premiar o penalizar a ningún usuario según a que contenidos a través de la red accedan, o desde que tipo de dispositivo naveguen. Todo tráfico de información deberá circular de forma transparente.
- **Derecho de acceso universal a internet (art. 81 LOPDGDD)**: toda persona tiene derecho a tener un acceso a internet de calidad independientemente de su situación geográfica, económica, personal, social e independientemente de su sexo o edad.

[12] La Lista Robinson: www.listarobinson.es

- **Derecho al olvido (art. 93 y 94 LOPDGDD)**: el interesado podrá exigir la supresión de sus datos personales que aparezcan en algún lugar de la red. Por ejemplo, en redes sociales o en motores de búsqueda.

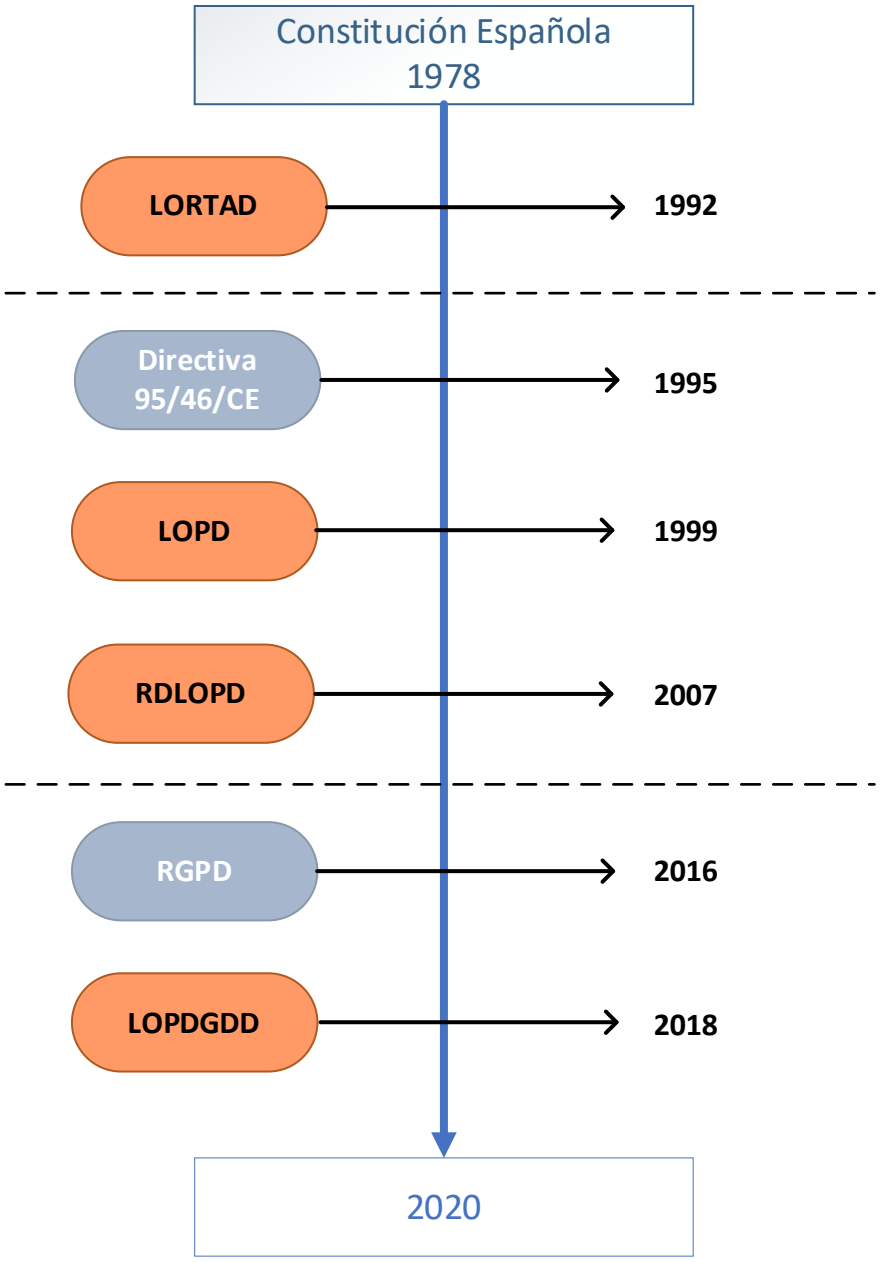

Figura 2: Leyes de Protección de Datos en España (Elaboración propia)

En la figura anterior, mostramos una línea temporal en la que situamos las diferentes normativas que hemos tenido en España relativas a la protección de datos y que hemos comentado a lo largo de este apartado anterior.

2.3 Implicaciones del RGPD

Una vez visto cómo ha ido evolucionando la legislación vigente entorno a la protección de datos personales, vamos a detallar qué nuevas normas ha impuesto el RGPD y a que artículos de la adaptación de nuestra LOPDGDD, hacen referencia. Veremos que estas normas vienen definidas por unos principios de protección de datos más explícitos. Aparecen novedades en los derechos de los interesados, se crean nuevas figuras con obligaciones concretas y requerimientos de seguridad, cambia la obligatoriedad de reportar brechas y fugas de información y también el régimen sancionador.

Primero repasaremos los derechos que podrán ejercer los usuarios sobre el tratamiento de sus datos personales y después las obligaciones que deberán poner en práctica las organizaciones para garantizar la protección de los datos personales de los interesados y de esa manera, poder demostrar cumplimiento.

2.3.1 Derechos de los interesados

A continuación, vamos a explicar en un lenguaje claro y conciso cuales son los principales derechos de los que disponen los interesados relacionados con la cesión de sus datos personales. Para ello nos apoyaremos en los artículos del “Capítulo III Derechos del interesado”, que comprende desde el artículo 12 hasta el artículo 23, del RGPD.

- **Derecho a la transparencia de la información (art. 12, 13 y 14 RGPD) (art. 11 LOPDGDD)**: antes de realizar cualquier cesión de datos personales, se le debería facilitar al interesado una información sencilla de comprender, en el mismo momento de recoger sus datos. En esta información debería aparecer la identidad del responsable del tratamiento, descripción del tratamiento que se les realizará a tus datos, la posibilidad de una cesión o transferencias a otros países de estos y todos los derechos que tiene el usuario sobre esos datos almacenados.
- **Derecho de acceso (art. 15 RGPD) (art. 13 LOPDGDD)**: haciendo uso de este derecho, podemos dirigirnos al responsable del tratamiento para confirmar cómo se están tratando nuestros datos y con qué finalidad. Cuáles son las categorías que se tratan, el tiempo durante el que se van a almacenar esos datos e información de la obtención de los datos si no han sido facilitados por el interesado. En caso de haber cesiones, conocer a quienes se les ha cedido.

- **Derecho de rectificación (art. 16 RGPD) (art. 14 LOPDGDD)**: este derecho nos permitirá revisar y actualizar nuestros datos cedidos si encontramos alguna incorrección en los mismos.
- **Derecho de supresión (art. 17 RGPD) (art. 15 LOPDGDD)**: como interesados, también podremos hacer uso de este derecho cuando consideremos que nuestros datos no se tratan acorde al fin con el que fueron recogidos o que se están tratando ilícitamente ("Licitud del tratamiento" art. 6 RGPD). Al solicitar la supresión, en caso de que el responsable del tratamiento haya cedido algunos datos personales, estará obligado a indicar a los terceros [18] responsables del tratamiento que eliminen cualquier referencia a los mismos, incluyendo cualquier lugar de la red (redes sociales, buscadores…). En la LOPDGDD los artículos 93 y 94 (derecho al olvido) que hemos nombrado anteriormente, complementan a su artículo 15.
- **Derecho a la limitación del tratamiento (art. 18 RGPD) (art. 16 LOPDGDD)**: con este derecho, podemos limitar o suspender el uso que se hace de nuestros datos personales.
- **Derecho a la portabilidad de los datos (art. 20 RGPD) (art. 17 LOPDGDD)**: el fin perseguido con este derecho es el de dar mayor control al interesado a la hora de querer transferir los datos personales a un tercer responsable de tratamiento. Podemos solicitar una copia de nuestros datos tratados por un responsable de tratamiento (responsable transmisor), en formato estructurado y de uso común, y pasarle directamente esos datos a otro responsable (responsable destino).
- **Derecho de oposición (art. 21 RGPD) (art. 18 LOPDGDD)**: usando este derecho, nos podemos oponer a que se realice un tratamiento de nuestros datos personales. Si por ejemplo se usan con otro fin sin haber dado consentimiento expreso de ello, o por otros motivos particulares que podamos acreditar.
- **Derecho a no ser objeto de decisiones basadas en tratamientos automatizados, incluida la elaboración de perfiles (art. 22 RGPD) (art. 11 LOPDGDD)**: de esta manera, el RGPD nos garantiza que nuestros datos no puedan ser solamente objeto de elaboración de perfiles [19] que puedan producir efectos jurídicos sobre nosotros. Este derecho no se aplicará si hemos dado consentimiento explícito para tal fin como parte de un contrato entre nosotros y el responsable del tratamiento.

Aunque no entraremos en detalle, si queremos remarcar que existen algunas limitaciones que pueden interferir en la aplicación de estos derechos anteriores, por

parte de los interesados. Estas limitaciones aparecen debidamente detalladas en el artículo 23 del RGPD.

A modo de resumen, podemos revisar la infografía "Los derechos que tienes para proteger tus datos personales"[13] que nos facilita la AEPD en su sitio web.

2.3.2 Deberes de las organizaciones

Dentro de las organizaciones, para adaptarse al RGPD se requerirán nuevas medidas que deberán ser llevadas a cabo por el responsable y el encargado del tratamiento [20] de datos personales. Para ver qué funciones tienen cada una de estas figuras dentro de una organización, podemos fijarnos en el "Capítulo IV Responsable del tratamiento y encargado del tratamiento" del RGPD que comprende desde el art. 24 al art. 31. No obstante haremos una breve explicación de ambos roles.

- **Responsable del tratamiento (art. 24 RGPD) (art. 28 LOPDGDD)**: es la figura que decide y define los mecanismos que hay que llevar a cabo para realizar las actividades de tratamiento de los datos personales de los interesados velando siempre por mantener la integridad y seguridad de estos. Podría existir un corresponsable de tratamiento (art.26 del RGPD) ya que varios responsables podrían juntarse para llevar a cabo un proyecto en común. Se debe acordar por escrito.
- **Encargado del tratamiento (art. 28 RGPD) (art. 33 LOPDGDD)**: suele ser una figura que trata los datos personales por cuenta del responsable, casi siempre un externo, y que aplicará las medidas que haya considerado el responsable acorde al tratamiento. Estas obligaciones o directrices deben acordarse por escrito, formalizadas en un contrato. Deberán llevar un registro de las actividades de tratamiento, así como determinar las medidas de seguridad que aplicarán a los tratamientos para proteger los derechos y libertades de los interesados. Los responsables sólo deberán elegir encargados que ofrezcan plenas garantías.

Antes de enumerar las medidas de responsabilidad activa que nos proporciona el RGPD para que las organizaciones puedan demostrar su cumplimiento, hay unos principios relativos al tratamiento de los datos personales que atañen principalmente a los encargados y responsables que lo llevan a cabo. Como nos indica el artículo 5 del RGPD estos son:

[13] Infografía AEPD: https://www.aepd.es/sites/default/files/2019-10/infografia-rgpd-derechos-ciudadanos-aepd.pdf

- Principio de **licitud, lealtad y transparencia** para que los datos sean tratados de manera lícita, leal y transparente.
- Principio de **limitación de la finalidad** para asegurar que los datos se recogen con fines determinados, explícitos y legítimos y que en ningún momento se podrán tratar de manera diferente a esos fines, a no ser que se traten con fines de investigación científica, estadísticos o de archivo de interés público.
    - A modo de ejemplo de vulneración de este principio, queremos resaltar una noticia de este pasado mes de Julio, en la que el Tribunal de Justicia de la Unión Europea ha declarado inválido el acuerdo establecido con Estados Unidos por el que se creó el escudo de la privacidad (o Privacy Shield) que establecieron el 2016[14], por tratar datos personales con otros fines a los determinados. Este acuerdo, proporcionaba los requisitos que debían seguir las empresas americanas para realizar actividades de tratamiento de datos de ciudadanos europeos, cumpliendo con los requisitos del RGPD. Desde ese momento, todos los datos transferidos internacionalmente que están bajo el paraguas de esa normativa son ilegales.
- Principio de **minimización de datos** para que la recogida de datos sea adecuada, limitada y pertinente a la finalidad del tratamiento.
- Principio de **exactitud** con el fin de evitar que los datos sean inexactos para cumplir con su tratamiento.
- Principio de **limitación del plazo de conservación** para garantizar que los datos solo se almacenan mientras dure su tratamiento para el que han sido recogidos.
- Principio de **integridad y confidencialidad** para que los responsables del tratamiento aseguren la seguridad de los datos frente a tratamientos no autorizados o pérdida de estos.
    - Otra noticia reciente que consideramos mencionar tiene que ver con la empresa Mercadona S.A. y la implantación de un sistema de reconocimiento facial, a principios del pasado mes de julio, en algunos de sus supermercados[15]. La AEPD ha abierto una investigación por las implicaciones que podría tener el tratamiento de estos datos biométricos, ya que son

[14] Invalidez del Escudo de la Privacidad: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales/comunicado-privacy-shield

[15] Mercadona y el reconocimiento facial: https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html

considerados datos sensibles y especialmente protegidos. La finalidad de este sistema, según dice Mercadona, es detectar a personas con órdenes de alejamiento contra la empresa o sus trabajadores y que por tanto tendrían prohibida la entrada al supermercado. Si revisamos el artículo 9.2 del RGPD, veremos que nos dice que se pueden hacer tratamientos de datos sensibles siempre que responda a un interés público esencial y proporcional al objetivo conseguido. La AEPD deberá sacar conclusiones y aportar una nueva visión que sirva como precedente a la utilización de este tipo de sistemas en nuestro país.

Aparte de estos seis principios, vemos que en el RGPD también se hace referencia al concepto de **responsabilidad proactiva**[16] como principio mediante el cual los responsables del tratamiento aplicarán las medidas necesarias para demostrar cumplimiento.

Para que las organizaciones puedan adaptarse al RGPD de una forma más sencilla, en los portales web de la AEPD, la AVPD y la APDCat, nos recomiendan algunas pautas que recogen las medidas de responsabilidad activa que establece la normativa. De esta manera se podrá garantizar el cumplimiento normativo.

Estas son las diez pautas que nos asegurarán cumplir con la normativa:

1) **Confeccionar un registro de las actividades de tratamiento (art. 30 RGPD) (art. 31 LOPDGDD).**

   Para poder empezar a realizar una actividad de tratamiento de datos personales, debe existir una base jurídica que la legitime. Las bases legales sobre las que se pueden realizar los tratamientos y que nos indica el artículo 6 del RGPD son:

   - **Consentimiento del interesado**. Nos sirve para adaptar un tratamiento anterior a la entrada en vigor del RGPD, ya que, desde ese momento, el consentimiento del interesado tiene que ser claro y explícito, no por omisión como anteriormente.
   - **Ejecución de una relación contractual**. A la hora de prestar o solicitar productos o servicios.

[16] Traducido como *Accountability* en inglés.

- **Cumplimiento de una obligación legal aplicable al responsable**. Obligaciones derivadas de la contratación de un trabajador por parte de una organización.
- **Protección de intereses vitales**. Para fines humanitarios, controles de epidemias, catástrofes naturales…
- **Cumplimiento de una misión realizada en interés público**. Para garantizar la seguridad ciudadana.
- **Interés legítimo del responsable o de terceros**. Esta base representa los casos más ambiguos, ya que permite un tratamiento de datos debidamente justificado por el responsable, sin requerir el consentimiento expreso del interesado y garantizando sus derechos y libertades.

Cada responsable y encargado del tratamiento, deberá llevar un registro de todas las actividades de tratamiento que se realicen bajo su responsabilidad, proporcionando así una gestión efectiva ante consultas de los interesados sobre la utilización de sus datos personales. La actividad deberá añadirse al registro previamente a su puesta en funcionamiento. Según el artículo 30 del RGPD, este registro contendrá:

- Nombre y datos de contacto del responsable, corresponsable, representante [21] del responsable, si los hubiera, y del DPD.
- Finalidad del tratamiento. Por ejemplo: gestión de recursos humanos, gestiones con proveedores, clientes, gestión económica, gestión de usuarios, gestión de quejas, videovigilancia, etc.
- Categoría de interesados y categoría de datos personales
- Categoría de destinatarios [22] de los datos personales, incluir terceros países u organizaciones internacionales.
- En caso de transferencias a terceros países, añadir la identificación del país u organización con la documentación de garantías adecuadas (art. 49.1 RGPD).
- Los plazos previstos para la supresión de los datos.
- Descripción de las medidas técnicas y organizativas de seguridad.

Según el artículo 30.5 del RGPD, estos requisitos anteriores, no se aplicarán a ninguna organización que tenga menos de 250 empleados. Sin embargo, en ese caso, igual se deberían cumplir si el tratamiento incluye datos sensibles, o existe

un riesgo elevado que pueda afectar a los derechos o libertades de los interesados.

Hemos elaborado documento para elaborar este registro que está disponible en el anexo I “Plantilla para el registro de actividades de tratamiento”.

2) Adecuar los métodos de recogida de datos de los interesados para informarles y así garantizar su derecho a la transparencia de la información (art. 12, 13 y 14 RGPD) (art. 11 LOPDGDD).

A la hora de obtener datos personales de los interesados, el responsable del tratamiento debe proporcionarles información clara y concisa del uso que se va a hacer de los mismos. En caso de que los datos hayan sido obtenidos a través de una cesión legítima y no por medio del interesado, el responsable informará en un breve plazo de tiempo al usuario sobre la obtención de estos. Siempre se tiene que poder acreditar que el deber de informar ha sido satisfecho, menos en algunos casos donde la comunicación con los interesados resulte imposible.

La recogida de datos se suele realizar a través de formularios impresos, formularios web, registros en aplicaciones, llamadas de teléfono, etc. Todos estos medios, deberán actualizarse y mostrar la siguiente información detallada de forma clara, concisa y con un lenguaje sencillo:

- **Responsable**. Se deberá informar sobre la identidad y los datos de contacto del responsable del tratamiento, o del Delegado de Protección de Datos si procede, incluyendo una dirección postal y electrónica.
- **Finalidad**. Añadir una descripción de los fines para los que se realizará el tratamiento de los datos personales proporcionados, incluyendo el plazo de conservación de estos.
- **Legitimación**. Indicaremos la base jurídica sobre la que se sustenta el tratamiento.
- **Destinatarios**. Si existe la previsión de realizar una cesión de datos, se informará sobre la identidad de los destinatarios, y otras normas aplicadas derivadas de esa cesión.
- **Derechos**. Informaremos textualmente de los derechos concernientes a los interesados y como puede ejercerlos.

- **Procedencia**. Solo incluiremos este apartado en caso de no haber obtenido los datos directamente del interesado. En él informaremos sobre el origen y como los hemos obtenido.

Las autoridades de control españolas nos recomiendan utilizar un modelo de información por capas representado en la tabla siguiente, para diseñar nuestra política de privacidad. Este enfoque consiste en presentar en la 1ª capa la información básica en el momento de realizar la recogida de datos y remitir a la 2ª capa con información más detallada donde se clarificará la información básica.

Apartado	1ª Capa (Información básica)	2ª Capa (Información detallada)
Responsable	Identidad	Datos de contacto
Finalidad	Descripción sencilla	Descripción detallada Plazos de conservación Automatizaciones, lógica aplicada
Legitimación	Base jurídica	Detalle de la base jurídica
Destinatarios	Previsión de transferencias o cesiones de datos	Destinatarios Decisiones de adecuación a la cesión, normas aplicadas
Derechos	Derechos del interesado	Cómo ejercerlos
Procedencia	Origen de datos (si no proceden del interesado)	Detalle del origen de datos

Tabla 1: Modelo de dos capas en la política de privacidad (Elaboración propia)

3) Adaptar los procedimientos para el ejercicio de los derechos de los interesados.

Facilitar el ejercicio de los derechos de los interesados estableciendo mecanismos que sean fáciles de utilizar. Por ejemplo, dedicar una dirección de correo electrónico o un formulario web para esa finalidad, que nos permita responder al interesado siempre dentro de los plazos marcados por el RGPD, es decir un mes, aunque prorrogable a dos meses más según la complejidad de las solicitudes.

4) Elaborar los contratos entre los responsables y los encargados del tratamiento.

Este documento supondrá un acuerdo o acto de encargo del tratamiento, entre responsables y encargados, y deberá contener toda la información relacionada con las actividades de tratamiento que se van a ceder.

Esta información estará formada por:

- **Instrucciones del responsable**. Se deben detallar de forma concreta las actividades de tratamiento que realizará el encargado, así como los datos que se le van a ceder. Si el encargado va a tener que realizar alguna cesión de datos, deberá constar también en el documento.
- **Deber de confidencialidad**. Se debe establecer un consenso para que todas las personas autorizadas a tratar los datos firmen un compromiso de confidencialidad. Este compromiso debe ser documentado y a disposición del responsable del tratamiento.
- **Medidas de seguridad**. Se indicará la obligatoriedad por parte del encargado de aplicar todas las medidas de seguridad necesarias para cumplir con el artículo 32 del RGPD. Tanto el responsable como el encargado deberán realizar un análisis de riesgos que les permitirán establecer las medidas de seguridad adecuadas para cumplir con sus respectivas funciones protegiendo los derechos de los interesados.
- **Régimen de subcontratación**. Para permitir una subcontratación con un tercero por parte del encargado del tratamiento, debe existir una autorización previa y por escrito del responsable del tratamiento. El subencargado deberá cumplir las mismas obligaciones y medidas de seguridad que el encargado en lo referente al adecuado tratamiento de los datos cedidos. Si el subencargado incumple sus obligaciones, la responsabilidad frente al responsable, será del encargado.
- **Derechos de los interesados**. Indicar de qué manera el encargado colaborará con el responsable para poder permitir el ejercicio de los derechos a los interesados y contestar a sus solicitudes. Se deberá especificar si esa tarea corresponderá al encargado llevarla a cabo, o este solamente desarrollará la función de comunicar los ejercicios de derechos al responsable. En caso de que el encargado la lleve a cabo, se establecerán la forma y los plazos para ello.
- **Colaboración en el cumplimiento de las obligaciones del responsable**. Debemos indicar como el encargado colaborará con el responsable para garantizar el cumplimiento de las obligaciones relacionadas con la notificación de brechas de seguridad a la AEPD y a los interesados, la implantación de medidas de seguridad, la realización de evaluaciones de impacto y la realización de consultas previas.

- **Destino de los datos al concluir la prestación**. Hay que especificar qué hará el encargado con los datos una vez realizada su función, pudiendo suprimirlos o devolverlos al responsable o a otro encargado que haya nombrado el responsable. También se añadirán los plazos para ello. No obstante, si por motivo legal se exige la conservación de los datos, si o sí, deberán ser devueltos al responsable.
- **Demostrar el cumplimiento al responsable**. El encargado pondrá a disposición del responsable toda la información necesaria para justificar su correcto cumplimiento normativo.

En el anexo I del documento de la AEPD "Directrices para la elaboración de contratos entre responsables y encargados"[17] podemos encontrar una plantilla para redactar el contrato.

5) Llevar a cabo un análisis de riesgos (art. 32 RGPD) (art. 28.2 LOPDGDD).

De esta manera, conoceremos si algunas actividades de tratamiento pueden conllevar riesgos para los derechos y libertades de los interesados y nos permitirá adoptar las medidas oportunas para tratar de minimizarlos. Incluiremos las medidas técnicas y organizativas más adecuadas en la empresa.

Este análisis de riesgos debería hacerse de manera periódica, sobre todo si vamos a introducir una nueva actividad de tratamiento que por el tipo de datos que se vayan a recopilar, pueda conllevar algún riesgo, teniendo en cuenta el principio de responsabilidad proactiva.

En la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD" que nos facilita la AEPD, observamos las 3 fases generales necesarias para llevar a cabo una gestión de riesgos de forma correcta.

[17] Directrices para la elaboración de contratos entre responsables y encargados: https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

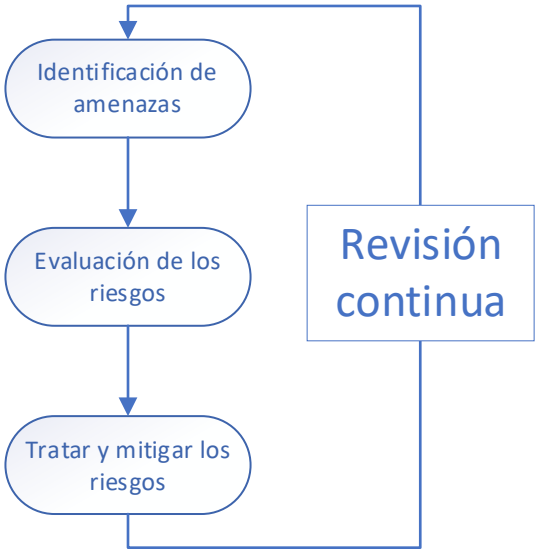

Figura 3: Etapas de la gestión de riesgos (Elaboración propia)

- **Identificar amenazas**. Estas se pueden clasificar en: acceso ilegítimo a los datos (confidencialidad), modificación no autorizada de los datos (integridad), eliminación de los datos (disponibilidad).
- **Evaluar los riesgos**. Para ello, hay que suponer que las posibles amenazas se van a materializar. Esto nos ayudará a determinar las consecuencias que podrían tener sobre los derechos y libertades del interesado, es decir el impacto que puede producir si la amenaza se cumple.
- **Tratar los riesgos**. Establecer mecanismos o medidas de control necesarias para mitigarlos.

Un poco más adelante explicaremos como realizar un análisis básico de riesgos sobre las actividades de tratamiento de datos que a priori no sean de carácter sensible y supongan un bajo riesgo para los derechos y libertades de los interesados.

6) Revisar las medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos (art. 32 RGPD).

Tras haber realizado un análisis de riesgos, es un buen momento para revisar los posibles puntos débiles, y ver como los podemos mejorar. Como responsables, es nuestra obligación garantizar la disponibilidad, integridad y confidencialidad de los datos de los interesados.

A veces, nos encontraremos con que implantamos medidas que pueden parecer suficientes, pero si no se aplican correctamente, pueden añadir más riesgo aún si cabe al tratamiento. De nada sirve proteger documentación con datos personales utilizando un armario con cerradura si a veces se nos olvida guardar las llaves y las dejamos puestas. Tampoco sirve proteger información con contraseñas si luego esta la dejamos apuntada en algún papel y no seguimos una política de mesas limpias.

Ahora que el teletrabajo ha cobrado mucho protagonismo, sería interesante mejorar en técnicas de destrucción de datos que ya no necesitemos tratar. Por ejemplo, garantizar la destrucción de la documentación en papel que puedan usar los trabajadores desde sus domicilios una vez procesada. Evitar que la acaben tirando a la basura creando un posible riesgo innecesario.

Dejando de lado los riesgos que pueda conllevar cualquier actividad de tratamiento, también existen otros riesgos potenciales inherentes a las personas, ya que, sin ser conscientes de ello, para los ciber atacantes son el eslabón más débil para conseguir información. Las organizaciones, como medida adicional de responsabilidad proactiva, deberían considerar tratar de concienciar a sus trabajadores para que estos no sean posibles víctimas de ataques de ingeniería social [23], como el que hemos visto recientemente que se ha llevado a cabo contra Twitter[18]. Para ello, el Instituto Nacional de Ciberseguridad (INCIBE), nos ofrece recursos y herramientas didácticas gratuitas como el Kit de concienciación para empresas[19].

Existen también procedimientos orientados a organizar la gestión de una organización en algunas de sus funciones como las Normas ISO, establecidas por el Organismo Internacional de Estandarización, que podríamos implantar en la nuestra para demostrar implicación, concienciación y previsión. Algunas de estas normas relacionadas con la seguridad de la información son:

- Norma ISO 27005 de Gestión de riesgos de la Seguridad de la Información. Indica cómo proceder a la gestión de los riesgos relativos a la información de una empresa. Esta norma se apoya en la ISO 27001 de Sistemas de Gestión de la Seguridad de la Información (SGSI) que nos indica los requisitos para llevarla a cabo.

[18] Ataque cibernético a Twitter: https://www.xataka.com/seguridad/todo-que-se-sabe-mayor-hackeo-a-twitter-historia-factor-humano-como-gran-problema-seguridad
[19] Kit de concienciación para empresas: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

- Norma ISO 31000 de Sistema de Gestión de Riesgos. Nos brinda un marco para la gestión de todo tipo de riesgos. Puede trabajar perfectamente con la ISO 27001.

7) Protección de datos desde el diseño y por defecto (art. 25 RGPD).

El responsable del tratamiento deberá tener siempre en mente el principio de responsabilidad proactiva y garantizar que los derechos y libertades de los interesados no se vean vulnerados, desde el inicio de la definición de las actividades de tratamiento, así como durante el tratamiento de los datos personales. Tendrá que garantizar que sólo se traten los datos necesarios para la finalidad por la que fueron recogidos.

Al inicio de este verano, la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) puso en funcionamiento, a modo de pruebas, una aplicación móvil para rastrear contactos de riesgo por COVID-19[20]. En el documento publicado, hacen referencia a la participación de la AEPD en el proyecto. La misma AEPD, mediante otro comunicado[21], lo desmiente argumentado que la implicación ha sido limitada y empezó una vez anunciado públicamente el proyecto, dando a entender que se implicó por las competencias que le atañen. El informe de réplica acaba con esta advertencia que queremos remarcar: «El Reglamento General de Protección de Datos no excluye la posibilidad de mejorar un tratamiento de datos en las etapas finales de su desarrollo, pero establece claramente que es el responsable de ese tratamiento quien debe tener en cuenta la protección de datos desde el inicio del diseño del proyecto».

8) Preparar los procedimientos y mecanismos necesarios de actuación ante la necesidad de notificar una brecha de seguridad (art. 33 y 34 RGPD) (art. 37 LOPDGDD).

Atendiendo al principio de responsabilidad proactiva, es necesario que el responsable tenga el registro de las actividades de tratamiento para poder saber inmediatamente que datos se han puesto en peligro, y un análisis de riesgos realizado que nos ayude a saber cómo de grave puede llegar a ser esta situación.

[20] Comunicado de la SEDIA: https://www.mineco.gob.es/stfls/mineco/prensa/noticias/2020/200623_np_gomera.pdf
[21] Réplica de la AEPD: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-sobre-la-participacion-de-la-aepd-en-la-app-de

Con esta información se debe trazar un plan de acción que nos ayude a detectar las posibles brechas.

Si se produce un riesgo probable para la seguridad de los datos o de los derechos de los interesados y se materializa la brecha de seguridad, el responsable debería poner en marcha el plan trazado para esa causa y tratar de resolverla minimizando las consecuencias que pueda tener. También está obligado a notificar esa brecha a la autoridad de control correspondiente en el plazo máximo de 72 horas a través de la Sede electrónica[22]. Para ese momento, es muy importante tener la mayor cantidad de información sobre lo ocurrido, es decir, conocer el origen, los tipos de datos afectados, que cantidad de datos, la procedencia, la intencionalidad… cuanta más información, mejor podremos abordar el problema. Si no tenemos un plan trazado, conseguir toda esta información en menos de 72 horas, puede ser muy complicado. Para que tengamos clara la información que necesitaremos documentar, la AEPD nos pone a disposición la "Guía para la gestión y notificación de brechas de seguridad[23]"

Habría que avisar a los supuestos afectados en caso de que la brecha acarreara un alto riesgo, con recomendaciones a seguir para minimizar el riesgo que les pueda proporcionar. Para ello se utilizará el canal habitual de comunicación con un lenguaje claro que les permita tomar las medidas pertinentes lo antes posible.

Si la brecha le ocurre a un encargado del tratamiento, este debe remitirla inmediatamente al responsable para que este tome las decisiones oportunas y proceda a comunicarse con la AEPD o con los interesados.

Ante esta situación, también se podrían producir demandas por una vulneración de los derechos de los interesados e incluso, si el riesgo ha afectado a más de uno, estas podrían venir en cascada, acarreando un coste en reputación y económico elevadísimo.

En definitiva, si nuestros protocolos son buenos, podríamos no tener que avisar si por ejemplo tenemos los datos cifrados o disipamos rápidamente el riesgo (art. 34 RGPD).

[22] Sede electrónica AEPD: https://sedeagpd.gob.es/sede-electronica-web/
[23] Guía para la gestión y notificación de brechas de seguridad: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad%20%281%29_0.pdf

Ante situaciones de posibles brechas de datos sensibles, sería totalmente recomendable disponer de la figura del Delegado de Protección de Datos, ya que los trámites con la autoridad de control se harían de forma rápida y concisa.

9) Realizar una evaluación de impacto de protección de datos (en adelante EIPD) tras revisar el resultado de un análisis de riesgos si fuera necesaria (art. 35 RGPD).

Una EIPD es un procedimiento que se realiza para identificar, controlar y mitigar los riesgos que puedan afectar a los derechos y libertades de los interesados, relacionados con las actividades de tratamiento de sus datos. Esta pequeña definición nos puede causar confusión a la hora de distinguir una EIPD de un análisis de riesgos. Aunque ambas herramientas tienen la finalidad de minimizar los riesgos y amenazas, el análisis de riesgos está más enfocado a las técnicas de protección de los datos que garanticen la integridad, confidencialidad y disponibilidad de estos y de la entidad que los trata. La EIPD, que incluye un análisis de riesgos en el proceso, está enfocada a garantizar que siempre se aseguren los derechos y libertades de los interesados ante riesgos elevados.

No siempre será necesario realizar una EIPD. Dependerá del resultado del análisis de riesgo que hayamos hecho sobre cada actividad de tratamiento de datos. Si tras este análisis, se observa que el riesgo es alto, llevaremos a cabo la EIPD, de lo contrario, si el análisis de riesgos previo indica que las actividades de tratamiento no presentan riesgos relevantes, no será necesario realizarla. Además, el RGPD en el artículo 35.3, nos remite a tener que realizarla en caso de tratarse de:

«*a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.»

A continuación, dedicaremos un epígrafe a explicar y detallar paso a paso cómo, el responsable del tratamiento puede llevar a cabo una EIPD.

10) Analizar la necesidad u obligación de designar un Delegado de Protección de Datos (en adelante DPD) (art. 37-39 RGPD) (art. 34-37 LOPDGDD).

La figura del DPD, se define como un elemento clave ya que, con sus conocimientos legales sobre la protección de datos, puede garantizar el correcto cumplimiento de la normativa en las organizaciones. Es un perfecto asesor para el responsable del tratamiento.

No todas las entidades tienen la obligación de tener un DPD asignado. Según el artículo 37.1 del RGPD, se designará cuando:

«*a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;*

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.»

La LOPDGDD complementa al RGPD añadiendo otros supuestos que concreta en su artículo 34.1 donde dice que se designará cuando se trate de las siguientes entidades:

«*a) Los colegios profesionales y sus consejos generales.*

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.»

Después de conocer en qué casos es obligado, si nuestra organización no está representada por ninguno de los artículos anteriores, y por tanto no tenga la obligatoriedad de disponer de DPD, si que es verdaderamente aconsejable por una serie de motivos. Una de sus funciones principales será tratar con las obligaciones legales en materia de protección de datos de la organización. Aconsejará y supervisará a la empresa respecto al cumplimiento normativo del RGPD.

La figura del DPD puede funcionar como un mecanismo extrajudicial para la solución de conflictos de protección de datos. Con el DPD la empresa puede ganar tiempo (2 meses) ante posibles denuncias por incumplimiento, ya que es el nexo de unión entre la empresa y la autoridad de control.

2.4 Análisis básico de riesgos

Una vez vistas las diez pautas recomendadas a seguir para demostrar cumplimiento normativo, vamos a detallar la pauta número 5 y explicar cómo llevar a cabo un análisis básico de riesgos. Decimos básico porqué está enfocado a aquellas actividades de tratamiento que a priori suponen un riesgo bajo para los derechos y libertades de los interesados. En caso de tratarse de datos de alto riesgo, como hemos comentado anteriormente, realizaríamos una EIPD. Para ello, estudiaremos las diferentes guías propuestas por las autoridades de control, referenciadas al final del documento, y trataremos de acercarlo al usuario de una forma más comprensible.

Como estamos aplicando el principio de responsabilidad proactiva, en el momento de realizar el análisis básico de riesgos, dispondremos del registro de actividades de tratamiento debidamente cumplimentado (descrito en la pauta número 1), ya que es fundamental para poder empezar a analizar los posibles riesgos. Con el registro cumplimentado podremos comparar las semejanzas entre diferentes actividades y así tratar de agruparlas para poder visualizar los tipos de riesgos comunes. De esta forma podremos establecer medidas de seguridad por defecto para varias de ellas a la vez.

El responsable del tratamiento debe asegurar el correcto cumplimiento normativo desde la recogida de los datos proporcionados por el interesado hasta su completa destrucción. Debido a esto, vamos a definir las diferentes fases del ciclo de vida por las que pasa cada actividad de tratamiento de datos.

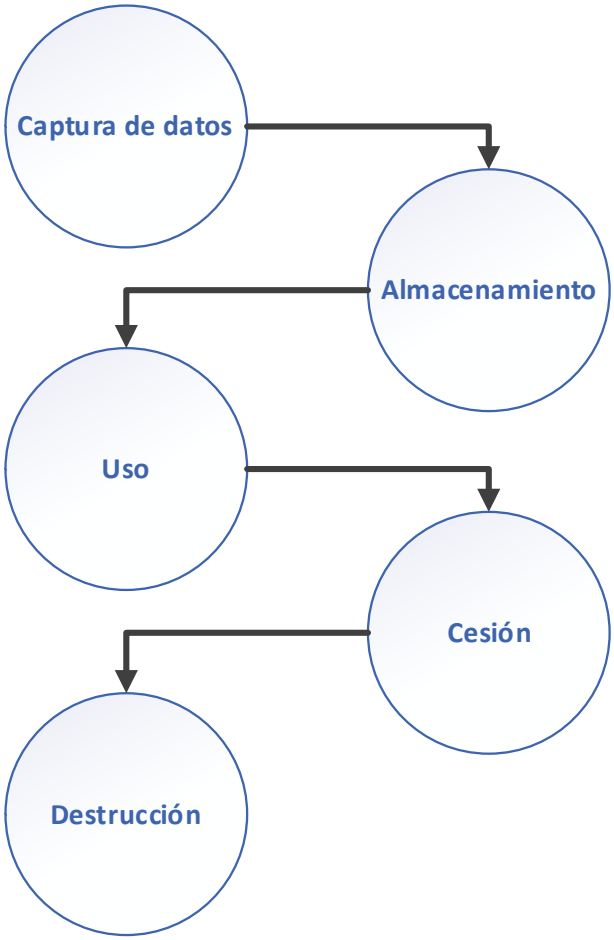

Figura 4: Fases del ciclo de vida de una actividad de tratamiento de datos (Elaboración propia)

1) **Captura de datos**: el interesado nos facilita sus datos personales a través del medio que hemos diseñado para su recogida.
2) **Almacenamiento**: cuando pasamos a introducir los datos obtenidos a nuestro sistema de archivado. Puede ser un sistema informático o en formato físico.
3) **Uso**: cuando procesamos esos datos almacenados para una finalidad específica.
4) **Cesión**: en el momento en que cedemos los datos a un tercero. Por ejemplo, cederlos a la administración o solicitar los servicios de un encargado de tratamiento.
5) **Destrucción**: es la fase del ciclo de vida en la que eliminamos definitivamente los datos. Ya hemos cumplido con la finalidad por la que fueron recogidos.

Dentro de cada una de las cinco etapas del ciclo de vida, intervienen los mismos cuatro elementos que pueden acarrear un riesgo.

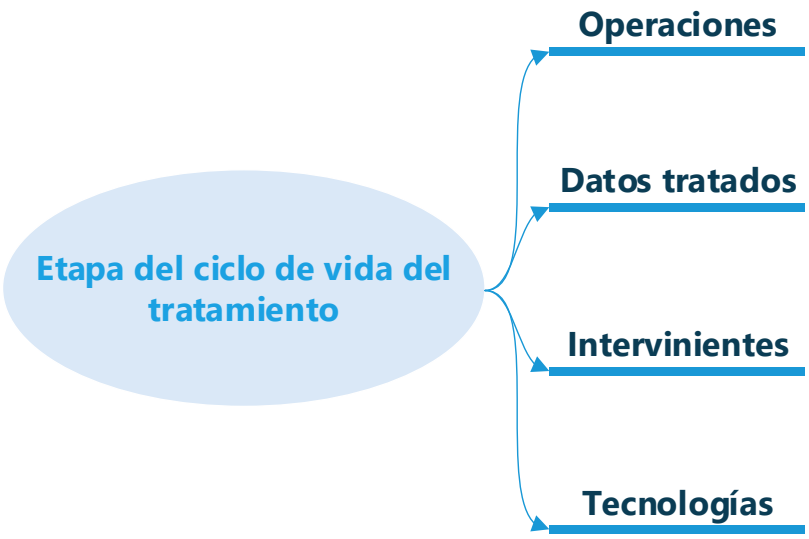

Figura 5: Elementos en cada etapa del ciclo de vida de los datos (Elaboración propia)

- **Operaciones**: procedimientos realizados en cada una de las fases del ciclo de vida sobre los datos de los usuarios. Por ejemplo, rellenar un formulario web, almacenamiento en una base de datos, elaboración de facturas, etc.
- **Datos tratados**: identificar el tipo de datos tratados en cada etapa. Los que se recopilan, los que se almacenan, los que se ceden y los que se gestionan.
- **Intervinientes**: personas físicas o jurídicas que intervengan a lo largo del ciclo de vida.
- **Tecnologías**: distintas tecnologías utilizadas en cada fase.

Para la recolección de los datos que acabamos de nombrar, se puede utilizar la siguiente tabla en la que aparecen las etapas del ciclo de vida cruzadas con los elementos de cada etapa.

		Elementos			
		Operaciones	Datos tratados	Intervinientes	Tecnologías
Etapas del ciclo de vida	Captura de datos				
	Almacenamiento				
	Uso				
	Cesión				
	Destrucción				

Tabla 2: Recogida de datos para identificación de posibles amenazas (Elaboración propia)

Como hemos explicado anteriormente, una gestión de riesgos completa consta de 3 etapas: identificación de amenazas, evaluación de riesgos y tratamiento y mitigación de estos. En este caso, debido a que este análisis básico de riesgos es para actividades de tratamiento cuyo nivel de riesgo inherente es medio o bajo, no hace falta realizar la etapa de la evaluación, pero igual los tenemos que identificar y tratar. Cada riesgo encontrado deberá tener asociada su medida de control para mitigarlo.

Para poder analizarlos, antes tenemos que definir como dimensionaremos los tipos de riesgos. Los riesgos que pueden afectar a los derechos y libertades de los interesados se pueden clasificar en:

- **Riesgos asociados a la protección de la información**: pueden poner en peligro la integridad, disponibilidad y confidencialidad de los datos.
- **Riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados**: el interesado no puede hacer uso de sus derechos correctamente por responsabilidad de la organización que trata sus datos.

Para cada una de las actividades de tratamiento, se debe analizar cuales son los riesgos inherentes y en cual de estos dos grupos deberían ir. Para ello podemos usar la siguiente tabla y de esta manera los riesgos y las medidas de control quedarán documentados.

	Tipología de riesgo	Riesgo	Medidas de control
Protección de la información	Integridad de los datos		
	Disponibilidad de los datos		
	Confidencialidad de los datos		
Cumplimiento de requisitos regulatorios	Garantizar ejercicio de derechos al interesado		
	Garantizar los principios del tratamiento		

Tabla 3: Identificación de riesgos y posibles medidas de control (Elaboración propia)

Como los riesgos pueden ir cambiando con el tiempo, es indispensable que el responsable realice un análisis de riesgos y revise las medidas de control de manera periódica.

2.5 Evaluación de impacto de protección de datos

Si el tipo de actividad de tratamiento supone un riesgo elevado para los derechos y libertades de los usuarios, el RGPD nos obliga a realizar una EIPD. Antes hemos explicado en qué consiste y cuál es la finalidad que persigue, pero ahora entraremos en detalles para conocer cómo llevarla a cabo.

El resultado de una EIPD será un informe que recogerá las características de las actividades de tratamiento llevadas a cabo, una identificación de los riesgos inherentes a esas actividades y las decisiones tomadas para mitigarlos.

Según el artículo 35.7 del RGPD, los puntos que debe incluir una EIPD son:

- Descripción sistemática de las actividades de tratamiento.
- Evaluación de la necesidad y proporcionalidad del tratamiento.

- Evaluación de los riesgos.
- Medidas para afrontar los posibles riesgos.

2.5.1 Fases de la EIPD

Para llevar a cabo la EIPD seguiremos un proceso sistemático que incluya los requisitos anteriores impuestos por el RGPD. A continuación, ilustramos las distintas fases de la metodología que utilizaremos.

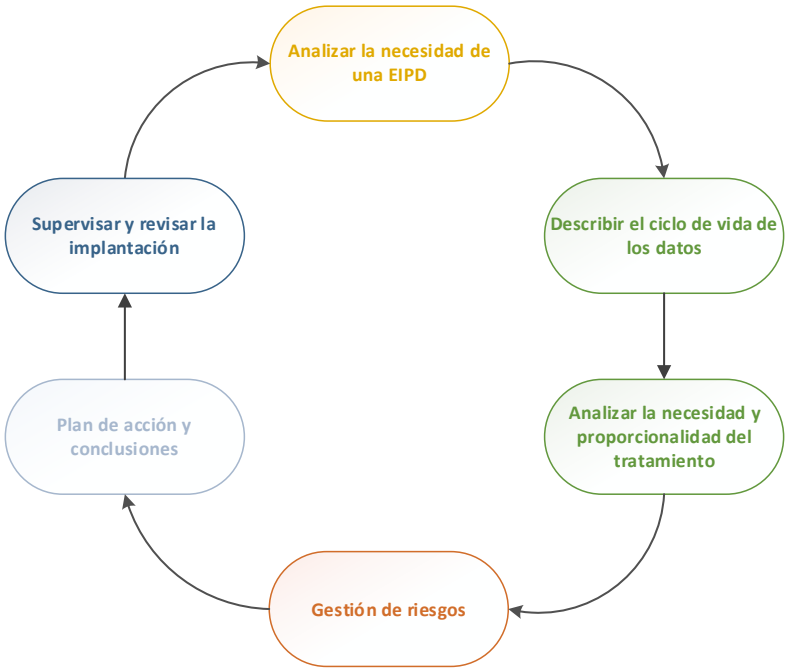

Figura 6: Fases a seguir en la Evaluación de Impacto de Protección de Datos (Elaboración propia)

1) **Analizar la necesidad de una EIPD**: incluimos esta fase porqué en caso de no ser necesaria, igualmente se debería justificar por qué motivo no se debe llevar a cabo.
2) **Describir el ciclo de vida de los datos**: tal y como hemos hecho en el análisis de riesgos, describiremos de forma detallada el ciclo de vida de los datos. Podemos utilizar la tabla que hemos propuesto en el punto anterior.
3) **Analizar la necesidad y proporcionalidad del tratamiento**: revisaremos el registro de actividades de tratamiento y analizaremos si cumple con sus principios y su finalidad.
4) **Gestión de riesgos**: realizaremos un análisis de riesgos completo, identificando amenazas, evaluando los riesgos y los trataremos y mitigaremos.

5) **Plan de acción y conclusiones**: Este será el resultado de la EIPD, un documento que contendrá todos los detalles de las fases anteriores y las medidas aplicadas para mitigar los riesgos y velar por los derechos y libertades de las personas físicas.

6) **Supervisar y revisar la implantación**: con la documentación generada no finaliza la EIPD. Esta requiere de un proceso de supervisión y revisión constante que garantice el cumplimiento normativo en caso de cambios producidos en el tratamiento. Es por esto por lo que esta fase se enlaza con la inicial en la figura anterior.

2.5.2 Actores principales en la EIPD

A la hora de realizar una EIPD, el principal ejecutor de esta será el responsable del tratamiento y no el DPD. No obstante, según el artículo 35.2, si se ha nombrado un DPD, este asesorará en el proceso de la EIPD al responsable del tratamiento, para llevarla a cabo de forma correcta. Además del responsable y en su caso el DPD, también puede intervenir el encargado del tratamiento.

Los roles que desempeñará cada actor durante todo el proceso, los hemos resumido en la siguiente tabla.

<table>
<tr><th></th><th>Responsable del tratamiento</th><th>Delegado de Protección de Datos</th><th>Encargado del tratamiento</th></tr>
<tr><td>Analizar la necesidad de EIPD</td><td rowspan="6">Responsable de llevarlas a cabo.

En caso de encargar un tratamiento, responsable de que se lleve a cabo y de validar su ejecución.</td><td rowspan="6">Debe ser consultado para que se lleven a cabo.

Debe ser informado sobre su realización.</td><td>-</td></tr>
<tr><td>Describir el ciclo de vida de los datos</td><td rowspan="4">Debe ser consultado para que se lleven a cabo.</td></tr>
<tr><td>Analizar la necesidad y proporcionalidad del tratamiento</td></tr>
<tr><td>Gestión de riesgos</td></tr>
<tr><td>Plan de acción y conclusiones</td></tr>
<tr><td>Supervisar y revisar la implantación</td><td>-</td></tr>
</table>

Tabla 4: Roles desempeñados por los actores que pueden participar en la EIPD (Elaboración propia)

2.5.3 Realización de la EIPD

Ya hemos definido la metodología a seguir y los actores que pueden intervenir con sus respectivos roles, ahora detallaremos cada una de las fases para poder llevar a cabo la EIPD.

1) **Analizar la necesidad de una EIPD.**

   En este punto, el responsable debería conocer la necesidad de realizar la EIPD tanto si es necesaria como si no. Para cumplir con el principio de responsabilidad activa, es necesario documentar cada una de las decisiones tomadas para proteger los derechos y libertades de los usuarios. En este caso, debería existir un documento que acredite la realización de la EIPD y por qué motivo. Actuando así siempre demostraremos compromiso con el cumplimiento normativo.

2) **Describir el ciclo de vida de los datos.**

   En el epígrafe del análisis básico de riesgos, hemos detallado como llevar a cabo este proceso. Cuando tengamos completada la tabla del ciclo de vida con un lenguaje comprensible y directo, pasaremos a analizar la necesidad y proporcionalidad de las actividades que están siendo tratadas.

3) **Analizar la necesidad y proporcionalidad del tratamiento.**

   En esta etapa, revisaremos nuestro registro de actividades de tratamiento y comprobaremos que se cumplen los principios del artículo 5 del RGPD relativos al tratamiento de los datos. También comprobaremos la licitud revisando las bases jurídicas de los tratamientos del artículo 6 del RGPD.

   Los datos deben ser tratados con la finalidad propuesta en su recogida, y no debe de existir otra manera de tratarlos que sea menos arriesgada para los derechos y libertades de los usuarios.

4) **Gestión de riesgos.**

   En este caso, no podemos suponer que el riesgo inherente del tratamiento de datos sea relativamente bajo como hemos hecho en el análisis básico de riesgos, y por tanto llevaremos a cabo las 3 etapas de la gestión de riesgo que hemos definido anteriormente. La finalidad perseguida será siempre valorar las

consecuencias negativas, es decir el impacto, que tendría una amenaza en caso de materializarse y mitigarlas.

Etapa de identificación de amenazas.

En la primera etapa de la gestión de riesgos, deberíamos contemplar, qué amenazas pueden conllevar las actividades de tratamiento que tenemos registradas y documentadas durante todo su ciclo de vida. Por ejemplo:

- **Desastres naturales**: incendios, inundaciones, etc.
- **Errores y fallos no intencionados**: borrado de información, fuga de información, etc.
- **Ataques intencionados**: ciberataques, robos, etc.
- **Incumplimiento del RGPD**: base legitimadora inexistente, cesión de datos sin documentar, no aplicar minimización de datos, etc.

Existirán más grupos de amenazas, aunque nosotros pondremos el foco en la tipología que hemos utilizado anteriormente en el análisis básico de riesgos. Nos centraremos en las amenazas que puedan conllevar riesgos sobre la integridad, disponibilidad y confidencialidad de los datos. Estas amenazas que hemos remarcado son:

- **Acceso ilegítimo a los datos (confidencialidad).**
  - Pérdidas de dispositivos electrónicos con información.
  - Fugas de información.
  - Ciberataques.
  - Uso ilegítimo de datos personales.
- **Modificación sin autorización de los datos (integridad).**
  - Suplantaciones de identidad.
  - Errores durante la captura de datos.
- **Borrado de los datos (disponibilidad).**
  - Fallo del equipo que suministra los datos.
  - Desastre natural.
  - Error humano o ciberataque de borrado.

Una buena práctica para identificar las posibles amenazas es respondiendo a preguntas relacionadas con la correcta aplicación de la normativa para garantizar los derechos y libertades de los interesados en todo momento. Por ejemplo, algunas preguntas podrían ser:

- ¿Los dispositivos que contienen información de los usuarios usan algún tipo de cifrado?
- ¿La información puede exponerse a externos durante el proceso de tratamiento?
- ¿Se puede limitar el acceso a la información?
- ¿Existen medidas de seguridad contra ciberataques?
- ¿Existen mecanismos de prevención ante desastres naturales?

Podemos elaborar una infinidad de cuestiones si preguntamos por aspectos que debemos cumplir. Lo importante es clasificarlas en aspectos comunes concretos de la normativa y tener siempre en cuenta sus respuestas para mejorar de forma continua el proceso de tratamiento de datos.

La posibilidad de que alguna amenaza se cumpla teniendo en cuenta el nivel de impacto sobre los derechos y libertades de las personas físicas, es a lo que llamamos riesgo. Es decir, en el supuesto caso de perder un dispositivo móvil con datos personales podría ocurrir que un externo acceda a información delicada de algún usuario. Que este externo tenga en su poder información sensible de los usuarios, podría llevar a cabo un uso que atente contra sus derechos y libertades. En este caso la **amenaza** sería perder el dispositivo móvil, el **riesgo** sería que un externo acceda a información confidencial de los usuarios y el **impacto** sería el posible daño moral que podría recaer sobre los usuarios tras una difusión de los datos.

Etapa de la evaluación de los riesgos.

Una vez identificadas las amenazas, pasaremos a valorar los riesgos. Para ello deberemos tener en cuenta el impacto posible y la probabilidad de que el riesgo se materialice. Para calcular la probabilidad y el impacto, nos basaremos en una escala de valores estandarizada basada en cuatro niveles (ISO 29134) aunque cada entidad puede utilizar una escala propia.

La escala utilizada para el cálculo de probabilidad se basará en estos cuatro niveles:

1) **Probabilidad despreciable**: posibilidad muy baja. Evento impredecible.
2) **Probabilidad limitada**: posibilidad baja. Evento ocasional.
3) **Probabilidad significativa**: posibilidad alta. Evento frecuente.
4) **Probabilidad máxima**: posibilidad muy elevada. Evento muy frecuente.

La misma escala utilizaremos para el impacto:

1) **Impacto despreciable**: impacto muy bajo. Evento con consecuencias de daño muy bajas para el interesado.
2) **Impacto limitado**: impacto bajo. Evento con consecuencias de daño menores.
3) **Impacto significativo**: impacto alto. Evento con consecuencias de daño elevado.
4) I**mpacto máximo**: impacto muy alto. Evento con consecuencias de daño muy elevadas contra el interesado.

Como vemos, el impacto va acompañado de un tipo de daño para el interesado. Los daños los podemos clasificar en:

- **Daño físico**: acciones que pueden ocasionar daños de integridad física. Por ejemplo, molestias, irritaciones, estrés, enfermedad, agresiones físicas, etc.
- **Daño material**: acciones que pueden acarrear una pérdida económica, de relación laboral, etc.
- **Daño moral**: acciones que pueden ocasionar daños mentales o morales. Por ejemplo, depresiones, fobias, persecución o acoso, etc.

Ahora que ya hemos cuantificado los impactos y las probabilidades de que las amenazas ocurran, pasaremos a cuantificar el riesgo.

Riesgo = Probabilidad x Impacto

Figura 7: Definición de riesgo en función del impacto y la probabilidad (Elaboración propia)

Para valorar el riesgo, utilizaremos la siguiente tabla que hemos elaborado fijándonos en la utilizada en la "Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD" de la AEPD donde cruzaremos los

cuatro tipos de probabilidad posible con los cuatro tipos de impacto. Para ello, a cada uno de esos tipos les asignaremos un valor del 1 al 4 donde 1 representa una probabilidad o impacto despreciable y el 4 representa a una probabilidad o impacto máximos. Esta tabla es conocida como la matriz de riesgos y consiste en establecer el producto del valor numérico del nivel de probabilidad por el nivel del impacto. Este valor numérico indicará el nivel de riesgo y se clasifica como:

- **Nivel bajo**: valores entre 1 y 2
- **Nivel medio**: valores mayores que 2 y menores o iguales a 6
- **Nivel alto**: valores mayores que 6 y menores o iguales a 9
- **Nivel muy alto**: valores mayores que 9

Probabilidad					
	Máxima (4)	4	8	12	16
	Significativa (3)	3	6	9	12
	Limitada (2)	2	4	6	8
	Despreciable (1)	1	2	3	4
		Despreciable (1)	Limitado (2)	Significativo (3)	Máximo (4)
		Impacto			

Tabla 5: Matriz de riesgos (Elaboración propia)

Esta tabla nos ayuda visualmente a identificar cual es la zona deseable en la que podemos contener un riesgo. Por ejemplo, si tenemos una amenaza con una probabilidad despreciable de que ocurra, y el impacto que tendría sobre los derechos y libertades del interesado fuera limitado, sería un resultado aceptable para ese riesgo. De lo contrario, si la probabilidad fuera limitada para un impacto también limitado, el riesgo sería medio y habría que tratar de mitigarlo.

Este ejercicio lo realizaremos para cada una de las amenazas documentadas.

Etapa de tratamiento y mitigación de los riesgos.

En esta última etapa de la gestión de riesgos, definiremos las medidas que sean necesarias para tratar los riesgos encontrados y mitigarlos. Para ello, las clasificaremos en medidas de:

1) **Reducción del riesgo**: estableceremos medidas que reduzcan los niveles de probabilidad e impacto asociados al riesgo.

2) **Retención del riesgo**: lo retendremos si el nivel de riesgo resultante es despreciable.

3) **Transferencia del riesgo**: podremos compartir un riesgo con una entidad externa, aunque esto puede acarrear otros riesgos. Hay que documentarlo y analizarlo.

4) **Anulación del riesgo**: si tras tratar de mitigar el riesgo, sigue siendo muy elevado, podemos optar por anular el tratamiento.

Algunas de las medidas posibles para la reducción del riesgo pueden ser de diferente índole:

- **Organizativas**: asociadas al funcionamiento interno de la entidad y a los procedimientos y medidas adoptadas para velar por los derechos y libertades de los interesados.
- **Legales**: asociadas a cumplir con lo establecido con la normativa.
- **Técnicas**: medidas que garanticen la disponibilidad, la integridad y la confidencialidad de la información almacenada en los sistemas de información.

Tras aplicar alguna medida para reducir el riesgo, deberemos estimar de nuevo la probabilidad y el impacto teniendo en cuenta los cambios acontecidos en los valores de las amenazas. Para ello volveremos a revisar la matriz de riesgos y comprobaremos si el nuevo valor de riesgo es aceptable o no hemos conseguido mitigarlo.

5) Plan de acción y conclusiones.

Una vez finalizado el análisis de riesgos, elaboraremos un plan de acción sobre el que plasmaremos todas las medidas de control que hayamos definido para tratar los riesgos que hayamos encontrado hasta reducirlos hasta un nivel considerable. También sacaremos conclusiones respecto a los resultados obtenidos. El plan de riesgos deberá contener además quien ha sido el responsable de la implantación de las medidas de control y el plazo en el que se han llevado a cabo.

Para llevar a cabo el plan de acción, deberemos tener en cuenta si la actividad de tratamiento sobre la que hemos hecho la EIPD es nueva o era ya existente. Si es nueva, la EIPD debería considerarse durante su fase de definición atendiendo al principio de privacidad desde el diseño y por defecto. En caso de realizar una EIPD sobre una actividad existente, si el valor del riesgo obtenido es alto, se deberá plantear un proyecto en el que se describan las medidas a llevar a cabo en un plazo máximo. Si se supera el plazo establecido, el responsable podrá interrumpir el tratamiento hasta que se apliquen las medidas correspondientes.

Si teniendo en cuenta la EIPD realizada vemos que somos incapaces, con las medidas que podamos aplicar, de aplacar el elevado riesgo que existe, tenemos que comunicarnos con la AEPD para solicitar una consulta (art. 36 del RGPD). Esto lo podemos hacer cumplimentando un formulario que encontraremos en su web[24]. De momento el tratamiento no podrá realizarse.

Si la EIPD ha sido satisfactoria y los niveles de riesgo son aceptables, se puede proceder con el tratamiento de datos.

6) Supervisar y revisar la implantación.

Por último, una vez realizada la EIPD, deberemos monitorizar que las medidas aplicadas se siguen llevando a cabo correctamente y corregir cualquier acción que pueda comprometer los derechos y libertades de las personas físicas.

En el anexo II de la memoria, hemos añadido una plantilla para llevar a cabo una EIPD. Hemos adaptado la plantilla proporcionada por la APDCat [25] a nuestra metodología.

2.6 Herramientas de las autoridades de control

Una vez detalladas todas las medidas de responsabilidad proactiva para demostrar cumplimiento normativo, revisaremos los portales de las distintas autoridades de control para ver que herramientas software proporcionan de manera gratuita, al responsable

[24] Consulta AEPD: https://sedeagpd.gob.es/sede-electronica-web/vistas/formConsultaPrevia/procedimientoConsultasPrevias.jsf
[25] Plantilla APDCat para la EIPD: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Plantilla-Avaluacio-Impacte-Proteccio-de-Dades.docx

del tratamiento, para ayudarle a la hora de aplicarlas. La AVPD, aunque tiene guías que hemos consultado, no tiene disponible ninguna herramienta software.

2.6.1 AEPD

En el portal web de la AEPD, aparte de muchas guías que hemos consultado, también tenemos la posibilidad de utilizar 4 herramientas web[26] que vamos a describir brevemente.

Facilita RGPD

Es una herramienta que sólo se debe utilizar por empresas que traten datos personales de escaso riesgo y consiste en rellenar unos formularios web respondiendo a preguntas que va realizando la aplicación.

La herramienta está orientada a generar la documentación necesaria adaptada a cada empresa, con las cláusulas informativas que habrá que añadir a los formularios de recogida de datos, con las cláusulas contractuales que se anexarán a la hora de encargar un tratamiento junto con el contrato con el encargado, el registro de actividades de tratamiento y medidas de seguridad recomendadas y los distintivos de zona videovigilada. La documentación generada deberá ser revisada y ajustada por la entidad que la utilice.

Gestiona EIPD

Esta herramienta está enfocada a realizar análisis de riesgos y EIPD. El funcionamiento es similar al de Facilita RGPD. Debemos ir rellenando unos formularios web y contestando a una serie de preguntas para poder llevar a cabo el proceso correctamente.

Al finalizar el proceso nos permite visualizar los riesgos que debemos mitigar. También podemos generar un informe de riesgos (si solo hemos hecho el análisis de riesgos) o generar el informe de la EIPD para seguir monitorizando el proceso.

Tanto Facilita RGPD como Gestiona EIPD no almacenan ningún dato introducido en sus formularios y por tanto no podemos retomar los procesos para revisarlos o completarlos con posterioridad.

[26] Herramientas web de la AEPD: https://www.aepd.es/es/guias-y-herramientas/herramientas

En el diagrama siguiente, mostramos cómo podemos utilizar estas herramientas según la AEPD para demostrar cumplimiento normativo a la hora de añadir una nueva actividad de tratamiento.

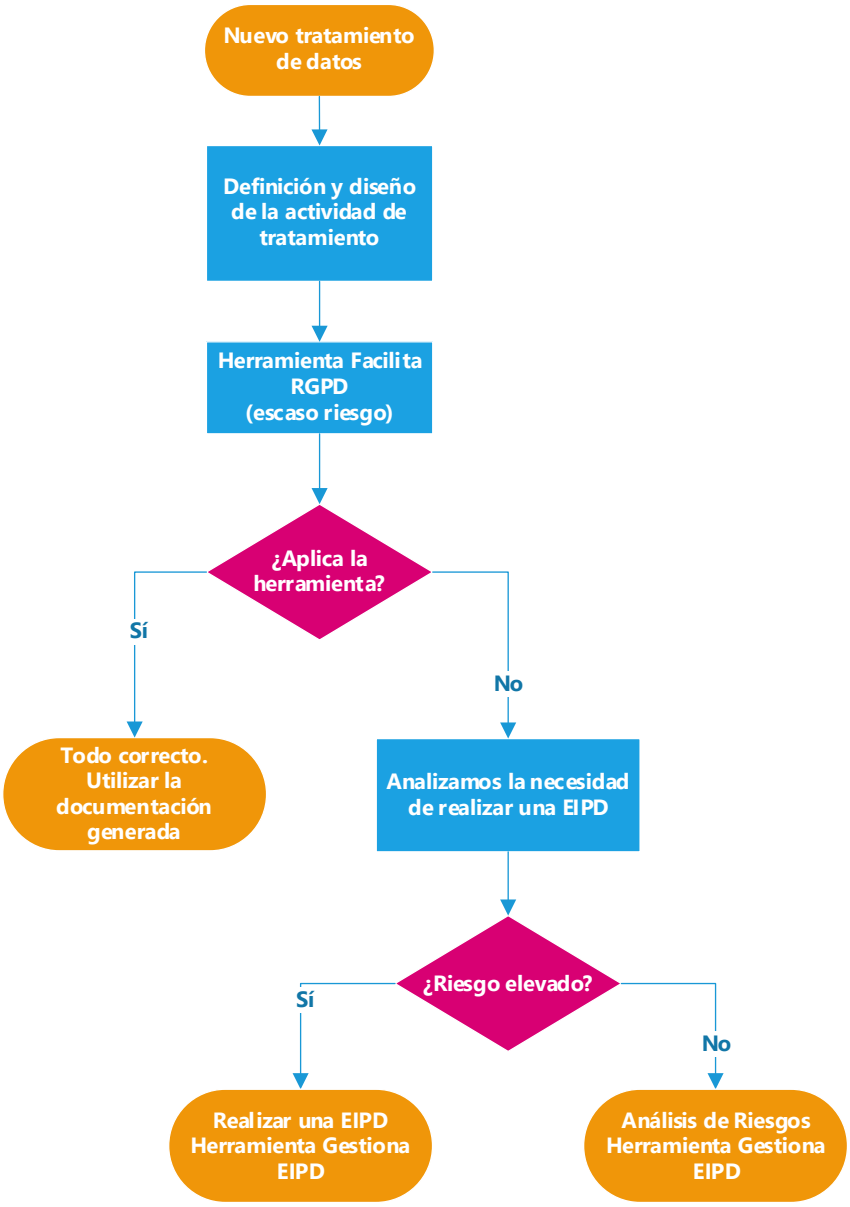

Figura 8: Herramientas AEPD para cumplimiento normativo (Elaboración propia)

Informa RGPD

Esta herramienta corresponde a un canal para prestar soporte a dudas respecto a la correcta aplicación del RGPD en las organizaciones o administraciones públicas. Las dudas pueden ser planteadas por los responsables, encargados o los DPD. Desde el

canal, nos remiten a todas las guías que ha desarrollado la AEPD con el fin de facilitar la comprensión de las medidas aplicables para garantizar el cumplimiento normativo.

Facilita EMPRENDE

Es una herramienta web similar a Facilita RGPD, pero en este caso orientada a emprendedores y startups debido a que los tratamientos tienen un componente innovador y se hacen uso de nuevas tecnologías, con los riesgos que estas pueden conllevar. En este caso se contemplan tratamientos que no sean de escaso riesgo.

Una vez concluido el proceso se genera el registro de actividades de tratamiento, una hoja de registro de incidentes para el caso de documentación de brechas de seguridad, política de información de dos niveles, cláusulas contractuales para añadir al contrato de encargo de tratamiento, política de cookies, directrices y recomendaciones.

2.6.2 APDCat

La web de la APDCat también contiene mucha información bien clasificada sobre la correcta aplicación de la normativa. Además, dispone de una herramienta software enfocada al registro de actividades de tratamiento llamada RAT[27].

RAT

Aunque el esfuerzo realizado para ponerle nombre a la aplicación parezca poco (Registro de Actividades de Tratamiento), nada tiene que ver con el dedicado a la creación de la herramienta. Se trata de una aplicación desarrollada para sistemas Windows muy poco pesada y bastante intuitiva de utilizar que trabaja en local sin conexiones a bases de datos externas. Por tanto, tenemos un control total sobre los datos introducidos en ella. El diseño y la experiencia de usuario es mejor que el que obtenemos con las herramientas de la AEPD, pero RAT sólo está orientada a crear, mantener y gestionar el registro de actividades de tratamiento. Nos permite dar de alta, de baja, modificar y generar informes de estos registros.

Es la herramienta perfecta para tener siempre controlado y actualizado nuestro registro de actividades de tratamiento.

[27] Herramienta RAT: https://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Aplicacio-per-gestionar-el-registre-de-les-activitats-de-tractament/

2.6.3 CNIL

La autoridad de control francesa también proporciona material de ayuda para los responsables de tratamiento en su web. Ha elaborado una plantilla para el registro de las actividades de tratamiento basada en Excel, una guía de cumplimiento normativo y una aplicación para realizar EIPD llamada PIA (*Privacy Impact Assessment*[28]).

PIA

De todas las herramientas que hemos visto, esta es la que mejor desarrollada está. Tiene una interfaz muy didáctica ya que integra una base de conocimientos con muchos conceptos relacionados con el RGPD que puedes ir consultando a medida que vas rellenando los formularios. De esa forma nos permite ir aprendiendo el reglamento mientras vamos introduciendo los datos. Con ella podemos realizar una EIPD desde la primera fase hasta la última.

Es multilenguaje[29] y multiplataforma[30] ya que está desarrollada sobre Electron[31], que es un *framework*[32] para desarrollos con JavaScript que permite que podamos desarrollar aplicaciones de escritorio basadas en tecnologías web. El problema es que las aplicaciones desarrolladas bajo esta tecnología suelen utilizar demasiados recursos del sistema mientras están en ejecución y esto suele afectar a la fluidez durante su funcionamiento.

2.7 Crítica a la situación actual

Llegados a este punto de la memoria, queremos remarcar las dificultades que nos hemos encontrado durante la fase de investigación para desarrollar esta guía que utilizarán los responsables del tratamiento. Partiendo de la base de que nuestro conocimiento sobre el RGPD era mínimo, necesitábamos aprender sobre metodologías y normativa para poder redactar esta guía de la manera mas clara posible.

Estando toda Europa al abrigo de la misma normativa de protección de datos, a veces daba la sensación, que la información obtenida para aprender sobre la correcta aplicación del RGPD en las organizaciones, era interpretada de diferentes maneras. Entendemos que el reglamento tiene laxitud en algunos puntos, permitiendo ciertas decisiones a los países miembros para que lo adapten un poco a su forma de entenderlo,

[28] Privacy Impact Assessment: Evaluación de impacto en su traducción inglesa.
[29] Desarrollada en varios idiomas, entre ellos el español.
[30] Funciona en diferentes sistemas operativos.
[31] Web del framework Electron: https://www.electronjs.org/
[32] Framework: «marco de desarrollo», (Linguee 2020).

pero lo que nos ha sorprendido, ha sido a la hora de revisar las guías de las diferentes autoridades de control españolas. Aunque en el fondo todas van de la mano, en las formas no. Esto puede llegar a confundir al usuario que está aprendiendo conceptos nuevos que son de obligada aplicación.

Dicho lo anterior, queremos lanzar esta reflexión: ¿por qué no se ha desarrollado un procedimiento claro para que todos los países de la unión apliquen el RGPD de la misma forma? Parece ser que resulta complicado unificar 27 leyes derivadas de la antigua Directiva.

2.8 Balance en estos dos años de funcionamiento

Consideramos acertado realizar un breve repaso a las impresiones de algunos profesionales durante estos 2 años desde su aplicación. Para ello nos hacemos eco de una entrevista que concedió el señor Marcos Judel, presidente de la Asociación Profesional Española de Privacidad (APEP)[33] a la revista digital CSO España en su número 48[34].

En su portada vemos un titular que nos da el mismo Marcos Judel «La privacidad no es un freno a la tecnología y la economía, sino una garantía de desarrollo», pero es en la sección "En primera persona" que comienza en la página 9, donde nos da sus impresiones relacionadas con el auge de aplicaciones telemáticas que han surgido a raíz de la pandemia del Coronavirus y que recogen datos personales relacionados con la salud y con la localización para controlar posibles focos de contagio. En su entrevista, comenta que, a la hora de desarrollar esas aplicaciones, se debería priorizar la protección de datos desde el diseño, con medidas técnicas de seguridad, transparencia y minimización de riesgos. La finalidad siempre debería ser determinar los riesgos que les puedan afectar a los usuarios y ponderarlos para cumplir sus objetivos. También hace referencia al principio de minimización de datos poniendo como ejemplo una aplicación de medición de temperatura corporal, donde no debería guardarse la temperatura diaria, sino avisar cuando se supere un umbral, ya que de lo contrario se podría aprovechar ese exceso de datos para elaborar perfiles personales.

La gente es cada vez más consciente sobre la privacidad, aunque en las empresas no ocurre exactamente lo mismo. Algunas se han tomado la adaptación a la nueva

[33] APEP: Entidad sin ánimo de lucro que nace fruto del interés y preocupación de un grupo de profesionales de diferentes sectores, dedicados a la privacidad y protección de datos. Inscrita en el Registro de Asociaciones del Ministerio del Interior núm. 593433.
[34] Revista CSO España, nº48: https://cso.computerworld.es/pubs/cso48/

normativa muy en serio, otras no tanto, dato que sorprende ya que el riesgo reputacional a la par que económico, puede ser muy alto. Una brecha de seguridad por una mala gestión hace que te puedas quedar sin clientes por la pérdida de confianza, a parte de las elevadas sanciones que puede conllevar.

La protección de datos se tiene que ver como una inversión, ya que el mundo está cada vez más digitalizado y conectado. Por este motivo, si no se hacen las cosas bien siendo proactivos, luego tocará ir poniendo parches. Para ello, muchas empresas tienen la figura del DPD que, junto con el principio de responsabilidad proactiva, ayuda a rebajar mucho las posibles sanciones por incumplimiento.

En la misma revista, en la sección “ciberseguridad” que empieza en la página 15, tenemos el artículo “GDPR, dos años de la norma que revolucionó la protección de datos” donde se hace un pequeño análisis numérico de estos 24 meses desde su aplicación.

«Es la primera vez en la historia que una ley afecta a toda la humanidad» nos dice José Luis Piñar, un jurista especializado en derecho digital. No le falta razón, ya se según el RGPD, cualquier empresa que trate datos de interesados europeos, deberá adaptarse esté donde esté, algo nada fácil. Se necesita un cambio de cultura reactiva a proactiva, aun sabiendo que una mala praxis pueda provocar una brecha de seguridad que acarree sanciones de hasta el 4% anual facturado con un máximo de 20 millones de euros.

A nivel interno, España parece que lo está haciendo bien:

- Media de incumplimiento por los profesionales.
  - Europa → 17%.
  - España → 11%.
- Notificaciones de seguridad en las primeras 48h.
  - Se han triplicado este segundo año (1.549 frente a 547).
- Resoluciones sancionadoras.
  - 338 el último año.
- Tiempos medios de resolución de sanciones.
  - Reducción del 29% en el último año.
- Tiempos de actuaciones de investigación.
  - Reducción del 22% en el último año.

- Reclamaciones de los ciudadanos.
  - 11.590 en el último año. Las más comunes:
    - Servicios de internet → 11%
    - Videovigilancia → 12%
    - Inserción indebida en ficheros de morosidad → 12%
    - Reclamación de deudas y publicidad → 9%
- Sanciones de mayor importe por áreas.
  - Directorios → 2,9 millones de euros
  - Telecomunicaciones → 641.000 euros
  - Contratación fraudulenta → 620.620 euros
  - Quiebras de seguridad → 460.000 euros
- Núm. de Delegados de Protección de Datos en 2019
  - 50.326
    - Sector privado → 44.069
    - Sector público → 6.257

Una última observación que nos gustaría aportar de este artículo y que nos invita a la reflexión, es un pequeño titular que nos deja Chema Alonso, gran experto en ciberseguridad, que dice «la gente tiene que saber cómo funciona el ecosistema actual de comercialización de datos. Hay todavía un gran desconocimiento y sobre todo despreocupación».

2.9 Propuesta de mejora y metodología a seguir

Una vez que hemos alcanzado el objetivo principal de este trabajo, desarrollando una guía para ayudar al responsable de protección de datos a la hora de aplicar el cumplimiento normativo y entender como llevar a cabo una EIPD, vamos a tratar de plantar la semilla de la que se nutrirá otro proyecto. El objetivo es aprovechar todo el conocimiento que hemos adquirido a la hora de realizar la guía y tras nuestro trabajo de investigación sobre las herramientas y contenidos proporcionados por las diferentes autoridades de control.

La propuesta será la creación de una herramienta software sobre la que poder unificar las diferentes herramientas vistas junto con la información relevante para cumplir con la normativa de protección de datos. De esta forma podremos evitar tener que revisar y utilizar guías y herramientas de fuentes distintas. Con ello ahorraremos tiempo de búsqueda y procesamiento de información al tener todo lo necesario en una aplicación.

Para ello, a continuación realizaremos un análisis básico de los requisitos que consideramos importantes, realizaremos un prototipado y comentaremos la funcionalidad básica que debería tener la aplicación a través de la especificación de sus casos de uso. Revisaremos las tecnologías utilizadas para su desarrollo y diseñaremos una interfaz básica para hacernos una idea de la estructura.

Todas estas propuestas serán susceptibles a modificación si los autores del proyecto continuista así lo consideran.

Las fases para llevar a cabo nuestra propuesta serán las siguientes:

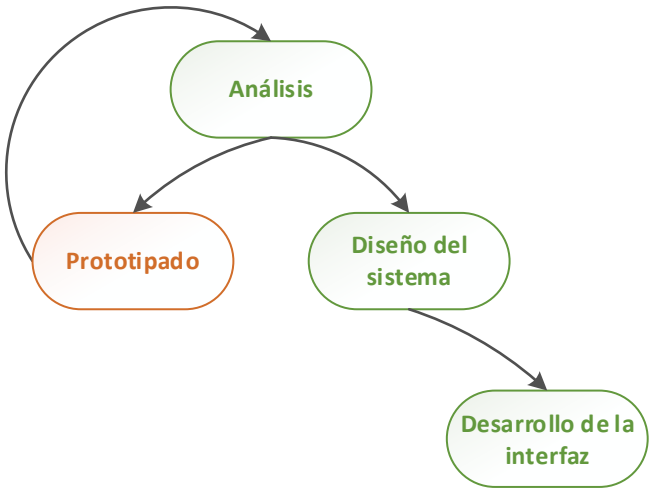

Figura 9: Fases para el planteamiento de la herramienta propuesta (Elaboración propia)

3. Análisis de requisitos

Una vez explicados los objetivos que pretendemos alcanzar con la propuesta que hemos realizado en el apartado anterior, empezaremos analizando qué requisitos consideramos imprescindibles para poderlos llevar a cabo. Tras la revisión de las herramientas de las autoridades de control, vamos a analizar aspectos relacionados con la seguridad y definiremos el comportamiento mediante un esbozo.

Cerraremos el epígrafe con la elaboración del plan de trabajo seguido en el TFG y realizaremos una estimación de costes mediante un presupuesto teniendo en cuenta todas las fases del plan de trabajo, no solamente la del desarrollo de la interfaz. De esta manera podremos monetizar el trabajo realizado.

3.1 Requisitos de seguridad

La aplicación propuesta deberá disponer de elementos de seguridad que la hagan tolerante a posibles riesgos. Por ejemplo, recomendamos que sea una aplicación portable, es decir, que sea autocontenida y que pueda ejecutarse directamente sin necesitar ningún proceso de instalación. Esto ayuda a que no tenga que ejecutarse en ningún servidor específico ni tenga que realizar ningún tipo de conexiones de transferencia de información. Llevará una base de datos embebida donde se almacenará la información que nos mostrará la aplicación, así como la información que nosotros introduciremos en ella a través de las distintas interfaces.

Al ser una aplicación portable, se podrá ejecutar directamente desde una memoria USB. Para ello recomendamos que la memoria esté debidamente cifrada y así asegurarnos que un posible extravío, no ponga en riesgo la confidencialidad de los datos.

El usuario principal de la herramienta deberá utilizar una contraseña robusta. Mínimo de 10 caracteres, combinando mayúsculas y minúsculas junto con números y símbolos.

La aplicación no contendrá ningún tipo de dato personal de ningún usuario creado, a excepción de una dirección de correo electrónico que se utilizará como identificador para entrar al sistema y para recuperar o reiniciar las contraseñas en caso de olvido. Aunque no se guarden datos personales, no hay que olvidar que podrá contener datos de medidas de seguridad empleadas para garantizar los derechos y libertades de los usuarios. Si estos datos caen en manos de ciberdelincuentes, podrían aprovecharlos para tratar de realizar ataques contra la compañía.

3.2 Boceto de la herramienta

Vistos los aspectos fundamentales relacionados con la seguridad, vamos a detallar el funcionamiento de la aplicación. Para tratar de ilustrar al máximo la descripción de las funciones principales que deberá poder realizar, hemos creado un esbozo de la interfaz de sus diferentes ventanas. Este boceto lo hemos llevado a cabo con la herramienta online y gratuita Mockingbird[35].

La primera figura que vemos corresponde al boceto de la ventana de inicio de la aplicación.

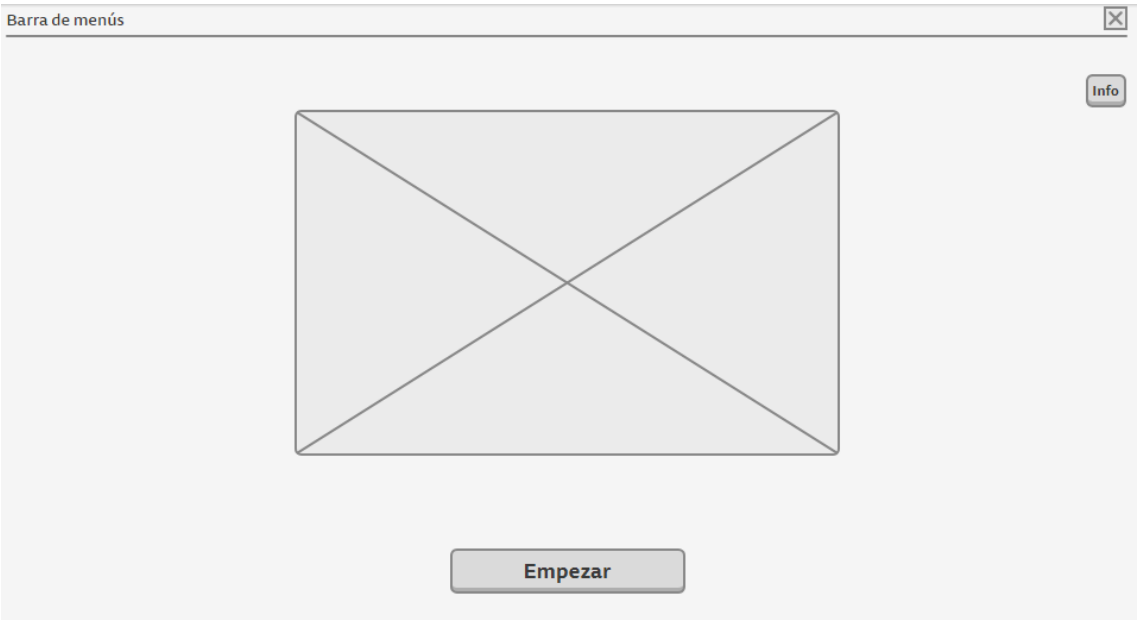

Figura 10: Boceto de la ventana inicial de la herramienta (Elaboración propia)

En ella mostraremos el logo de la aplicación, la **barra de menús**, y dos botones. El botón "**Info**" mostrará información adicional que pueda ser de interés para el usuario. El botón "**Empezar**" nos llevará a la ventana del panel de herramientas, que observamos en la siguiente imagen.

35 Sitio web de Mockingbird: https://gomockingbird.com/

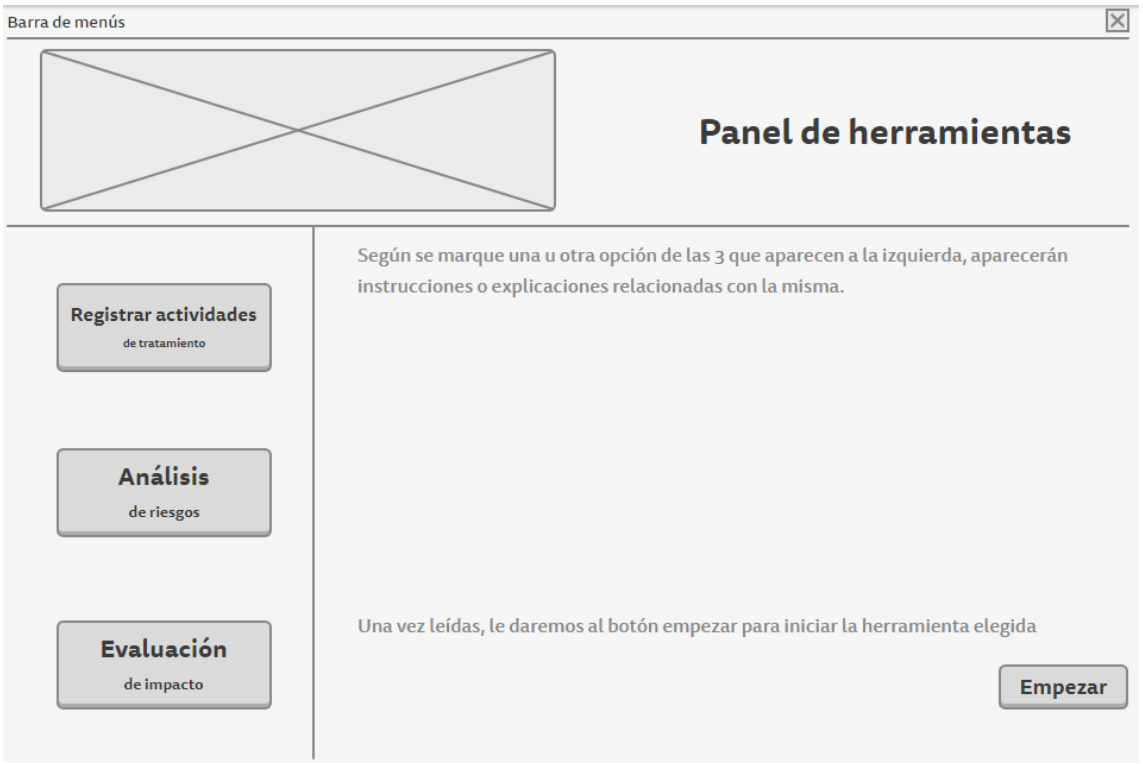

Figura 11: Boceto de la ventana del panel de herramientas (Elaboración propia)

Esta será la ventana principal, el panel de herramientas de la aplicación. En ella, podremos seleccionar una de las tres funciones que queramos llevar a cabo en ese momento. Podremos elegir entre confeccionar un **registro de actividades de tratamiento**, realizar **un análisis de riesgos** o llevar a cabo una **evaluación de impacto**.

Según la opción marcada, en el panel central nos aparecerá una descripción con información sobre su proceso y las indicaciones necesarias para saber cuando debemos usarla.

Una vez que estamos seguros de querer ejecutar la opción que hemos marcado, pulsaremos el botón "**Empezar**". Esto nos llevará a otra ventana cuyo boceto lo vemos representado en la siguiente figura.

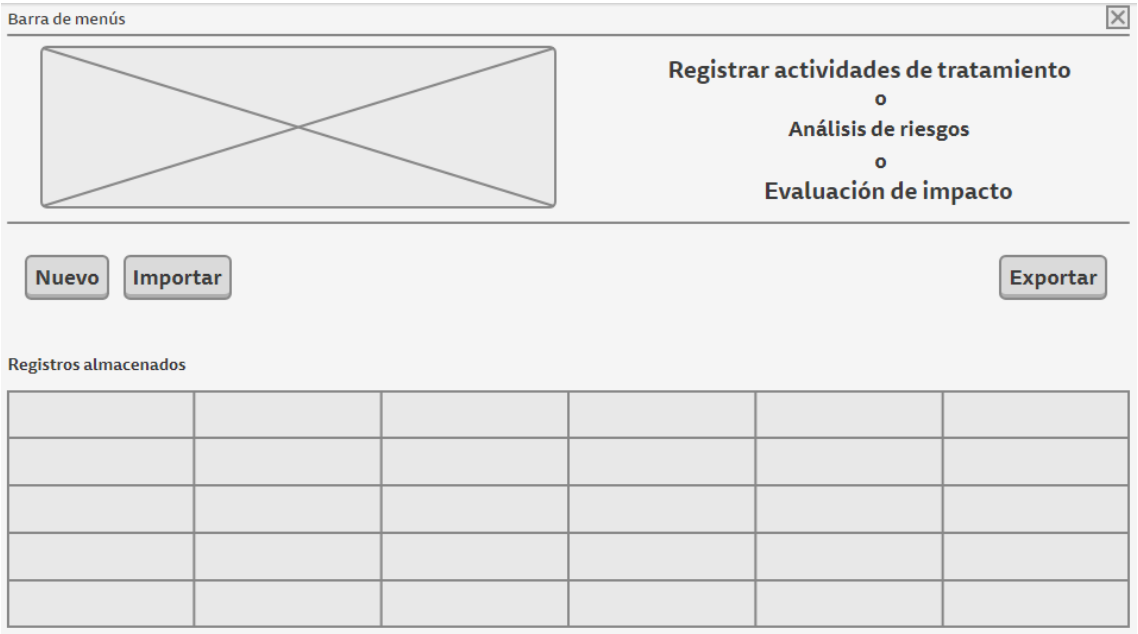

Figura 12: Boceto de la ventana principal de la herramienta seleccionada (Elaboración propia)

Con el fin de reutilizar código, la interfaz principal de la ventana que representa cada una de las tres funciones anteriores, será bastante parecida. Según la opción elegida, en la parte superior derecha, sólo aparecerá su título correspondiente y no los tres como vemos aquí.

En esta ventana tendremos un *grid*[36] central donde se nos mostrarán los diferentes registros que hayamos guardado previamente al haber utilizado la herramienta (cada ventana verá únicamente su tipo de registro). Si es la primera vez que la usamos, el grid aparecerá vacío.

La funcionalidad de los botones en esta interfaz es la siguiente:

- Botón "**Exportar**": en caso de tener algún registro en el grid, podremos seleccionarlo y exportarlo para guardarlo en el soporte que consideremos.
- Botón "**Importar**": si previamente hemos exportado algún registro, pulsando este botón, seremos capaces de cargarlo de nuevo a la herramienta. De esta forma lo veremos en el grid.
- Botón "**Nuevo**": si es la primera vez que ejecutamos esta función y no tenemos ningún fichero para importar, pulsaremos este botón para empezar con el proceso de captura de datos de la herramienta, como se muestra en la siguiente imagen.

[36] Grid: «Parrilla o cuadrícula», (Linguee 2020).

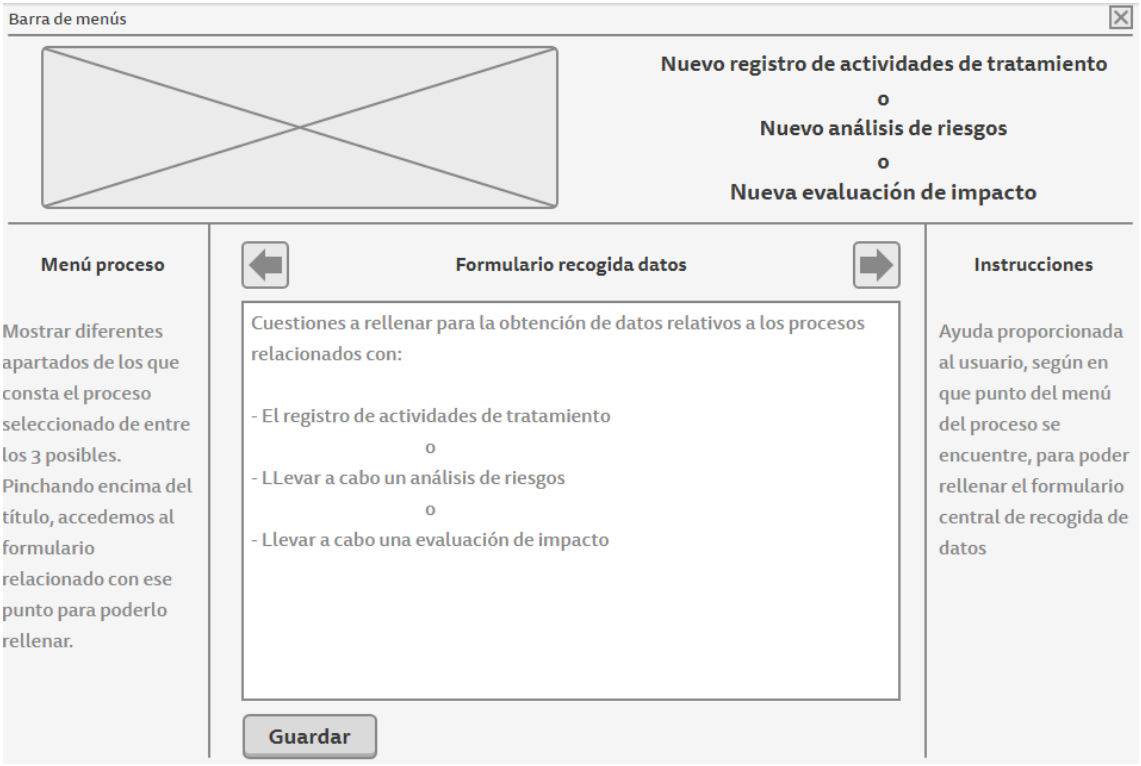

Figura 13: Boceto de la ventana del formulario de datos de las herramientas (Elaboración propia)

Al seleccionar el botón nuevo, para cualquiera de las tres funciones principales de la herramienta, mostraremos esta ventana mediante la que le introduciremos los datos a la aplicación rellenando los formularios que nos vayan apareciendo.

Vemos que esta ventana, a parte del panel superior que contiene el título, tiene otras tres secciones claramente diferenciadas. La sección de la izquierda contendrá una especie de panel de navegación o menú del proceso, que contendrá una referencia a las diferentes fases que habrá que completar. Siempre seremos conocedores de cual es la fase en la que nos encontramos. El área del centro será la que utilizará el usuario para introducir los datos a la aplicación a través de los formularios que nos mostrará la aplicación. El marco de la derecha mostrará indicaciones y definiciones de conceptos relacionados con el cumplimiento normativo. De esta manera, la herramienta, le facilitará la labor de comprensión e introducción de datos al usuario.

En la parte superior del panel central, están los **botones en forma de flecha** que nos permitirán avanzar o retroceder por las diferentes fases del formulario que aparecen en el panel de navegación.

Cuando hayamos acabado de introducir todos los datos necesarios, pulsaremos el botón "**Guardar**". De esta manera se almacenarán los datos introducidos en la base de datos. Actualizaremos el grid mostrando el nuevo registro. En caso de no haber

finalizado con la introducción de datos, podremos retomarla cuando consideremos oportuno.

3.3 Plan de trabajo seguido del TFG

Dentro del epígrafe del análisis de requisitos hemos considerado conveniente cuantificar el tiempo dedicado al desarrollo de este trabajo. Para ello lo hemos dividido en 8 fases diferentes que mostramos en el siguiente diagrama de Gantt junto con el tiempo dedicado a cada una de ellas. La fecha de inicio del proyecto fue el 11/05/2020 y la fecha de finalización el 8/08/2020 con un total de 358h de dedicación a una media de 4h diarias.

Id.	Nombre de tarea	Duración
1	Planificación del proyecto	28h
2	**Realización del proyecto**	**330h**
3	Fase de requisitos normativos UPV	28h
4	Fase de investigación	140h
5	Fase de análisis de la solución	62h
6	Fase de diseño y desarrollo	56h
7	Fase de redacción conclusiones	16h
8	Revisión de la memoria y resumen	28h

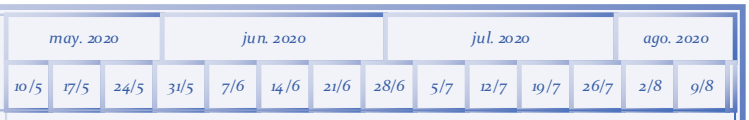

Figura 14: Duración de las fases del proyecto (Elaboración propia)

Aunque son 8 las fases definidas, la mayoría de ellas pertenecen a la fase de realización del proyecto, ya que la primera fase (**planificación del proyecto**), estaba enfocada a establecer los objetivos que debíamos alcanzar, como alcanzarlos y que criterios seguir para lograrlos.

Como hemos comentado, la fase 2 (**realización del proyecto**) en sí es una generalización de la unión de todas sus fases hijas. La primera de las fases hijas es la fase 3 (**requisitos normativos UPV**) cuya importancia era absoluta. No podíamos empezar a realizar un trabajo académico de esta índole sin conocer toda la normativa exigida por la Universitat Politècnica de València y por la Escola Tècnica Superior d'Enginyeria Informàtica.

La fase 4 (**investigación**) ha sido a la que le hemos dedicado un mayor número de horas, al tratarse de un trabajo basado en leyes y normativas. Si nos fijamos en las referencias bibliográficas que aparecen antes del glosario, nos podremos hacer una idea de la cantidad de información procesada.

La quinta fase (**análisis de la solución**) incluye el tiempo dedicado a analizar los requisitos necesarios de la herramienta propuesta para su completo desarrollo en un futuro proyecto.

La fase 6 (**diseño y desarrollo**) comprende la dedicación necesaria para completar los puntos 4 y 5 de la memoria. En ellos explicamos como debería llevarse a cabo la herramienta y su funcionalidad.

Para completar la séptima de las fases (**conclusiones**), hemos revisado todo el documento y hemos reflexionado sobre los objetivos alcanzados aportando nuestra valoración personal.

Para terminar, hemos dejado madurar la memoria durante un tiempo en el que hemos ido realizando pequeños ajustes y **revisiones**. Como parte final del proyecto, hemos escrito el **resumen**, ya que consideramos que debe ser lo suficientemente completo para poder captar la atención del lector al tratarse del fragmento más leído de cualquier TFG.

3.4 Presupuesto

Ahora que ya hemos cuantificado el tiempo dedicado al trabajo, vamos a monetizar esas horas teniendo en cuenta el salario medio estimado de un ingeniero informático en España según Indeed[37] que es de unos 27.406€ brutos al año. Esto equivale a unos 2.283€ brutos mensuales.

Durante un mes trabajamos 40h semanales repartidas en 4 semanas y 2 días aproximadamente, que equivalen a unas 176h. Por tanto, el coste por hora aproximado sería de unos 13€ brutos. Teniendo en cuenta que el tiempo total dedicado ha sido de 358h, el coste total del trabajo es de unos 4.654€ aproximadamente.

[37] Media salarial ingeniero informático en España: https://es.indeed.com/salaries/ingeniero-inform%C3%A1tico-Salaries

4. Diseño del sistema

Una vez que ya hemos planteado los requisitos mínimos que deberá cumplir la herramienta, vamos a definir los aspectos técnicos necesarios para poderla desarrollar en el siguiente proyecto. Comenzaremos recomendando que arquitectura del sistema implantar a la hora de desarrollar la aplicación. Detallaremos los casos de uso y expondremos las tecnologías a utilizar. En el epígrafe anterior hemos conocido qué aspectos debía cubrir esta propuesta de herramienta y en este apartado vamos a ver cómo cubrirlos.

4.1 Arquitectura del sistema

Con el objetivo de reutilizar código, de estandarizar el desarrollo y de limitar las dependencias entre los objetos de la aplicación, vamos a proponer desarrollar la herramienta basándonos en una arquitectura de 3 capas. La separación entre capas funciona a través de peticiones siguiendo un modelo parecido al cliente-servidor.

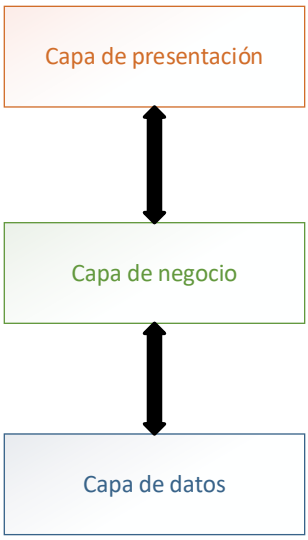

Figura 15: Arquitectura de 3 capas (Elaboración propia)

En la **capa de presentación** se añadirá toda la funcionalidad referente a la interacción entre el usuario y la propia aplicación. En esta capa es donde se desarrollan las interfaces junto con las validaciones de datos introducidos por el usuario, a través de las cuales se realizarán llamadas a procedimientos de la capa de negocio.

En la **capa de negocio**, se desarrollará el núcleo principal de la aplicación. En ella se ejecutarán los procedimientos que vengan desde la capa de presentación y se

devolverán las respuestas adecuadas según sus reglas predefinidas. Esta capa también tiene comunicación directa con la capa de datos.

La última de las tres capas, **la capa de datos** es la que se encarga de proporcionar persistencia a los datos. Su principal función es almacenar y responder con datos a la capa de negocio. Es la única que puede acceder directamente a esta información que estará almacenada en un servidor de bases de datos, ficheros, etc.

4.2 Detalle de funcionalidad y casos de uso

Con el fin de mejorar un poco más la funcionalidad de la herramienta después de haber realizado la fase de análisis de requisitos y de prototipar la aplicación, hemos añadido nuevos comportamientos cómo son la generación de informes que nos puedan requerir para demostrar cumplimiento normativo y la posibilidad de mostrar enlaces de interés donde el usuario pueda conocer de primera mano cualquier novedad en la normativa.

A continuación, vamos a detallar el funcionamiento de la aplicación basándonos en el análisis de sus casos de uso. Entendemos los casos de uso como un mecanismo que nos permitirá comprender los requisitos que deberán tener las interacciones del usuario con la aplicación. De esta forma comprenderemos mejor las dependencias funcionales entre las diferentes ventanas y añadiremos una visión secuencial a los diferentes procesos que se ejecutarán durante su utilización.

A la hora de empezar a utilizar la aplicación, será necesario un **registro del usuario**. En ese registro guardaremos solamente su correo electrónico, ya que no es necesario conocer ningún dato personal más. Una vez creada su cuenta, podrá **iniciar sesión** o **recuperar su contraseña** en caso de haberla olvidado. Para ello el sistema deberá **validar** que el usuario existe.

Una vez iniciada la sesión, el usuario podrá elegir que **herramienta** utilizar. Para ser más esquemáticos, hemos abreviado los nombres de las herramientas principales. Al registro de actividades de tratamiento lo llamaremos **RAT**, al análisis básico de riesgos lo llamaremos **ABR** y a la evaluación de impacto de protección de datos, **EIPD**. Como el proceso de funcionamiento de estas tres herramientas es similar, hemos agrupado sus casos de uso. En cada una de estas herramientas, el usuario podrá **crear**, **importar**, **modificar**, **exportar** o **borrar un registro**. En el caso de la modificación, la exportación o el borrado, deberemos comprobar que **existe** al menos **un registro**. Para crear o

modificar un registro, será necesario lanzar la ventana del **formulario de recogida de datos**.

Una de las dos herramientas que hemos incluido tras la fase de análisis, es la de **generación de informes**. A través de ella, podemos generar **informes** relacionados con las **RAT**, **ABR** y **EIPD** que hayamos realizado y también, imprimir plantillas de los **contratos entre los responsables y encargados**, documentación relacionada con la **videovigilancia** y la **política de privacidad** para mostrársela al usuario a la hora de proceder a la recogida de sus datos.

También podremos acceder a **enlaces de interés** para estar al corriente de posibles comunicados de las autoridades de control relacionados con la protección de datos.

Toda esta funcionalidad la hemos definido en el diagrama de casos de uso que mostramos a continuación.

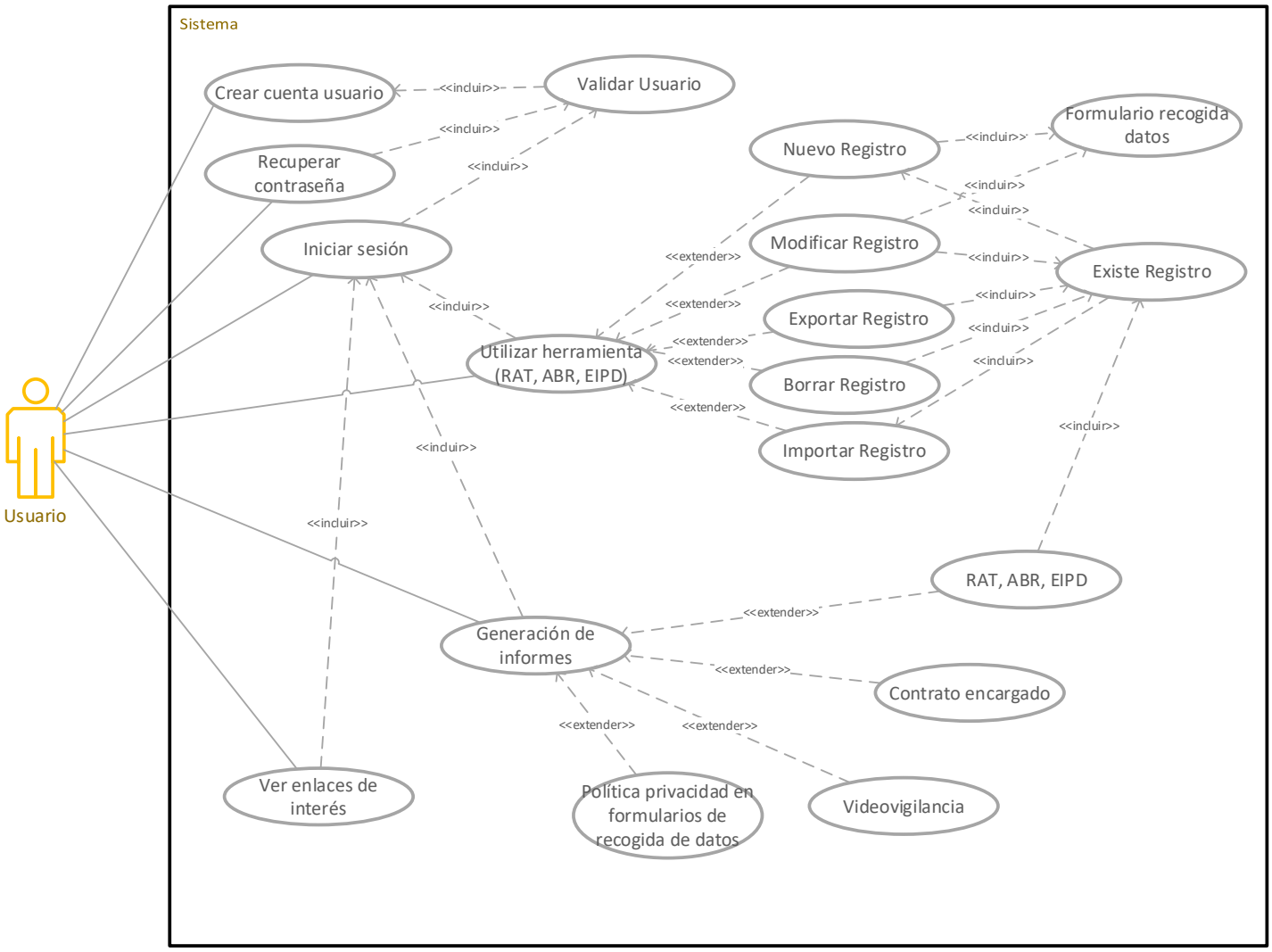

Figura 16: Diagrama de casos de uso de la herramienta (Elaboración propia)

4.3 Tecnologías utilizadas

Para llevar a cabo el desarrollo de la interfaz que veremos en el siguiente punto, nos hemos apoyado en las siguientes herramientas o tecnologías.

Como entorno de desarrollo nos hemos instalado **Visual Studio 2019**. Hemos utilizado la versión "Community" que ofrece una licencia gratuita para uso no comercial.

Para crear las interfaces de las ventanas, nos hemos basado en los formularios básicos, conocidos como **WinForms**, que son los más utilizados durante la programación en **Visual C#**. Usando estos formularios podemos crear ventanas con muchísima facilidad ya que trabajan bajo la filosofía WYSIWYG[38].

Con el fin de modernizar un poco la interfaz y disponer de iconos diferentes, nos hemos descargado una extensión para Visual Studio llamada **FontAwesome.sharp**. Con esta extensión, podemos acceder a una gran colección de iconos con solo introducir un nombre identificativo. En la web de FontAwesome[39] podemos ver las referencias de estos iconos para poderlos utilizar.

Como no queríamos diseñar una interfaz de una aplicación sin nombre, le pusimos uno y diseñamos su logo utilizando la aplicación para Android llamada **LogoMaker**[40].

Figura 17: Logo de la aplicación Mitiga2 (Elaboración propia)

[38] Acrónimo de What You See Is What You Get. En español significa: Lo que ves es lo que obtienes.
[39] Sitio web de FontAwesome: https://fontawesome.com/
[40] LogoMaker App para Android: https://play.google.com/store/apps/details?id=com.irisstudio.logomaker&hl=es

5. Desarrollo de la interfaz

En este apartado, vamos a mostrar las interfaces que hemos desarrollado utilizando las tecnologías mencionadas. Resulta bastante curioso ver como se puede ir adaptando el comportamiento y el diseño de una aplicación software desde su fase de análisis de requisitos hasta su fase de implementación.

En el apartado 3.2, hemos explicado el funcionamiento que pensábamos alcanzar con esta aplicación, ahora vamos a revisar como aplicarlo sobre una interfaz real y no sobre un boceto.

La imagen que aparece a continuación corresponde a la ventana de **inicio** de la aplicación. Durante la etapa del boceto, no hemos definido los procesos de crear un usuario ni de recuperar contraseñas.

Figura 18: Ventana de inicio de sesión de la aplicación (Elaboración propia)

Una vez iniciada la sesión, vemos que aparte de las 3 herramientas planteadas en el boceto, desde la ventana del panel de herramientas, podemos acceder también a la generación de informes y a la parte de los enlaces de interés. También hemos añadido datos referentes al inicio de sesión del usuario y 3 iconos en la parte superior derecha cuya funcionalidad es:

- 🛠 → Si lo pulsamos volvemos al panel de herramientas.
- ℹ → Mostramos información relevante sobre la aplicación
- ✉ → Pinchando sobre él, se nos abrirá nuestro cliente de correo predefinido para poder enviar un email con fallos o sugerencias.

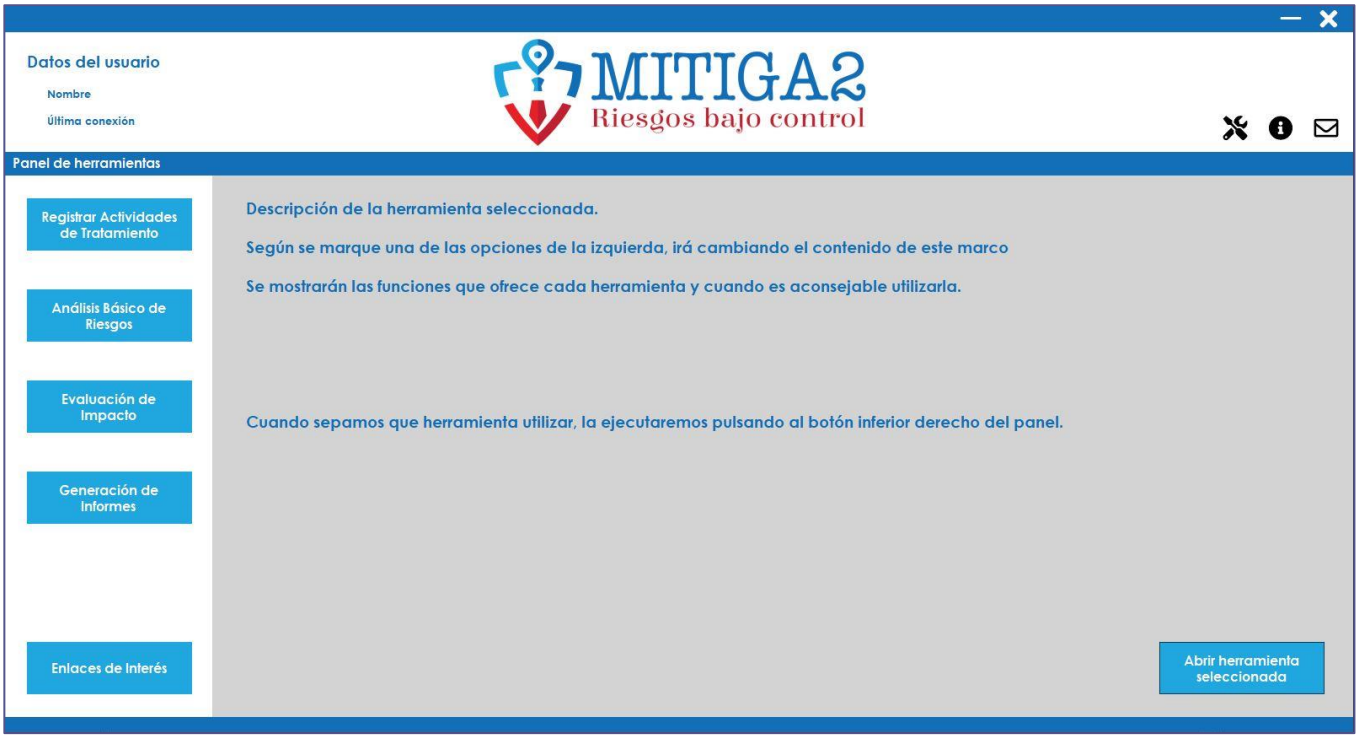

Figura 19: Ventana del panel de herramientas de la aplicación (Elaboración propia)

Para la herramienta de **generación de informes** no hemos diseñado ninguna interfaz, ya que consideramos que al no haber seguido un proceso estándar como si que lo hemos hecho con el registro de actividades de tratamiento, con el análisis de riesgos y con la EIPD, es mejor que determinen la funcionalidad los compañeros que continúen con el desarrollo de la herramienta en otro proyecto. En el caso de los **enlaces de interés**, la información se mostraría en la parte central del panel de herramientas.

Una vez seleccionada una de las tres herramientas principales, se mostrará la siguiente ventana, adaptada para cada caso.

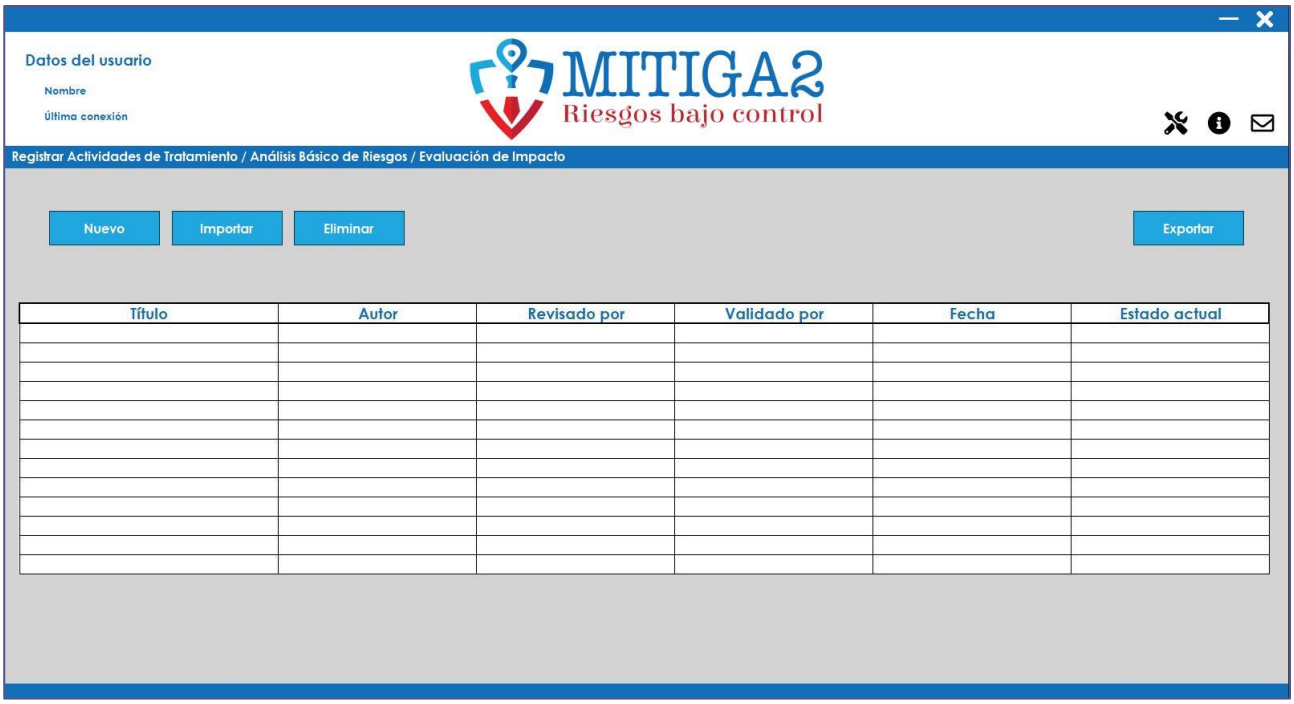

Figura 20: Ventana principal de las herramientas RAT, ABR y EIPD (Elaboración propia)

En esta ventana, lo único que añadimos respecto al diseño del boceto, es el botón **eliminar**. De esta forma, si nos situamos sobre un registro que aparezca en el grid, podemos eliminarlo. Al pulsar el botón nuevo, se nos abrirá la siguiente ventana.

Figura 21: Ventana de recogida de datos de las herramientas RAT, ABR y EIPD (Elaboración propia)

Como hemos explicado durante el diseño del boceto, esta ventana nos permitirá recoger toda la información proporcionada por el usuario y guardarla en nuestra aplicación. La ayuda y las fases del proceso es evidente que cambiarán acorde a la herramienta seleccionada. No se mostrará la misma ayuda para un ABR que para un RAT o EIPD.

6. Conclusión

A la vista de que cada vez más objetos traen tecnología incorporada que les permite intercambiar datos entre ellos, nosotros debemos ser más proactivos y estar alerta sobre los datos que cedemos. Es por esto por lo que, a lo largo de la memoria, hemos insistido sobre la capacidad de aplicar medidas de seguridad preventivas que puedan proteger la información personal de los usuarios.

Tras realizar un breve repaso a los mecanismos legales empleados durante las últimas décadas, sobre la protección de la privacidad de los usuarios y de sus derechos y libertades, hemos analizado las novedades que nos ha aportado la entrada en vigor del RGPD.

Con el fin de que los responsables de protección de datos de las distintas organizaciones puedan garantizar el cumplimiento normativo, hemos establecido un decálogo de pautas que les servirán de Guía. En este decálogo, se incluye como realizar los análisis de riesgos y las evaluaciones de impacto de protección de datos.

Para que nos demos cuenta de lo importante que es dejar de ser una sociedad que pone parches a sus problemas en lugar de tratar de adelantarse a ellos y prevenirlos, hemos ido relacionando noticias de actualidad con diferentes conceptos normativos aprendidos. Parece ser que tras estos dos años y poco de la aplicación del reglamento, muchos de los usuarios y organizaciones no son todavía conscientes del problema que puede acarrear una mala gestión de los datos.

Como objetivo final y que será el objetivo principal de otro proyecto, hemos propuesto el desarrollo de una herramienta software que sirva de ayuda para los responsables de protección de datos, explicando las características básicas que debería contener y el diseño de su interfaz.

El desarrollo del TFG sobre esta temática tan de actualidad nos ha removido la conciencia y nos ha mostrado lo mediocres que nos podemos sentir ante una mínima filtración de nuestra privacidad. Muchas veces esto es debido a que, desde las instituciones más importantes de un país, no se le da la relevancia que requiere a la protección de los datos personales. Hemos visto que la AEPD y el gobierno de España no han estado totalmente sincronizados a la hora de desarrollar la aplicación de los rastreos de la COVID-19. Si los propios gobiernos no tratan de involucrarse en el ámbito tecnológico pudiendo demostrar confianza con medidas preventivas convincentes, la sociedad no se tomará la protección de datos en serio.

Como dijo Tom Wheeler, un político estadounidense, en una conferencia de ciberseguridad sobre transparencia, comunicación y conflictos, a veces tenemos la sensación de que «nos estamos enfrentando a problemas tecnológicos del siglo XXI, discutiéndolos en términos del sigo XX y proponiendo soluciones del siglo XIX»[41]. La política no avanza a la par que las necesidades tecnológicas de los ciudadanos.

[41] Conferencia de ciberseguridad y comunicación: https://www.cnbc.com/video/2017/10/09/cambridge-cyber-security-summit-transparency-communication-and-conflict.html

7. Referencias

Agencia Española de Protección de Datos, 2018. *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento*. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf [Consulta: julio 2020].

Agencia Española de Protección de Datos, 2018. *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*. Disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-rgpd-para-responsables-de-tratamiento.pdf [Consulta: junio 2020].

Agencia Española de Protección de Datos, 2019. *Guía para el ciudadano*. Disponible en: https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf [Consulta: mayo 2020].

Agencia Española de Protección de Datos, 2018. *Guía para el cumplimiento del deber de informar*. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-modelo-clausula-informativa.pdf [Consulta: junio 2020].

Agencia Española de Protección de Datos, 2018. *Guía para la gestión y notificación de brechas de seguridad*. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf [Consulta: julio 2020].

Agencia Española de Protección de Datos, 2019. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf [Consulta: mayo 2020].

Agencia Española de Protección de Datos, 2018. *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf [Consulta: mayo 2020].

Agencia Española de Protección de Datos, 2018. *Listado de Cumplimiento Normativo*. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf [Consulta: mayo 2020].

Agencia Española de Protección de Datos, 2019. *LOPD: Novedades para el sector privado*. Disponible en: https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-sector-privado.pdf [Consulta: junio 2020].

Agencia Española de Protección de Datos, 2018. *LOPD: Novedades para los ciudadanos*. Disponible en: https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-ciudadanos.pdf [Consulta: junio 2020].

Agencia Vasca de Protección de Datos, 2019. *Adecuación de PYMES y profesionales al Reglamento General de Protección de Datos en ocho pasos*. Disponible en: https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/AVPD-Adecuacion_PYMES_a_RGPD_en_8pasos-v.1-es.pdf [Consulta: julio 2020].

Autoridad Catalana de Protección de Datos, 2019. *Avaluació d'impacte relativa a la protecció de dades*. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Guia-Practica-avaluacio-impacte-proteccio-de-dades-2019.pdf [Consulta: mayo 2020].

Autoridad Catalana de Protección de Datos, 2019. *Plantilla d'avaluació d'impacte relativa a la protecció de dades*. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/Plantilla-Avaluacio-Impacte-Proteccio-de-Dades.docx [Consulta: julio 2020].

BBC NEWS, Redacción, 2019. Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios. *BBC News Mundo* [en línea]. 24 de julio de 2019. Disponible en: https://www.bbc.com/mundo/noticias-49093124 [Consulta: junio 2020].

CABALLERO VELASCO, María Ángeles y CILLEROS SERRANO, Diego, 2019. *Ciberseguridad y transformación digital. Cloud, Identidad Digital, Blockchain, Agile, Inteligencia Artificial…* Madrid: Grupo Anaya. ISBN 9788441541627.

Convenio 108 del Consejo de Europa. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. *Boletín Oficial del Estado*, 15 de noviembre de 1985, núm. 274. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 [Consulta: mayo 2020].

Convenio Europeo de Derechos Humanos, adoptado por el Consejo de Europa el 4 de noviembre de 1950. Disponible en: https://echr.coe.int/Documents/Convention_SPA.pdf [Consulta: mayo 2020].

Declaración Universal de los Derechos Humanos. Adoptada y proclamada por la Asamblea General de la ONU en su resolución 217 A (III), de 10 de diciembre de 1948. Disponible en: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf [Consulta: mayo 2020].

España. Constitución Española. *Boletín Oficial del Estado*, 29 de diciembre de 1978, núm. 311. Disponible en: https://www.boe.es/eli/es/c/1978/12/27/(1)/con [Consulta: mayo 2020].

España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Boletín Oficial del Estado*, 31 de octubre de 1992, núm. 262, p. 37037-37045. Disponible en: https://www.boe.es/eli/es/lo/1992/10/29/5 [Consulta: mayo 2020].

España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, núm. 298. Disponible en: https://www.boe.es/eli/es/lo/1999/12/13/15/con [Consulta: mayo 2020].

España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294. Disponible en: https://www.boe.es/eli/es/lo/2018/12/05/3/con [Consulta: mayo 2020].

España. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. *Boletín Oficial del Estado*, 25 de junio de 1999, núm. 151, p. 24241-24245. Disponible en: https://www.boe.es/eli/es/rd/1999/06/11/994 [Consulta: mayo 2020]

España. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletín Oficial del Estado*, 19 de enero de 2008, núm. 17. Disponible en: https://www.boe.es/eli/es/rd/2007/12/21/1720/con [Consulta: mayo 2020].

Fundación del español urgente. Macrodatos e inteligencia de datos, alternativas a big data. *Fundeu BBVA* [en línea]. 7 de febrero de 2013. Disponible en: https://www.fundeu.es/recomendacion/macrodatosalternativa-abig-data-1582/ [Consulta: mayo 2020].

INCIBE, 2019. Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. *INCIBE* [en línea]. 5 de septiembre de 2019. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse [Consulta: Julio 2020]

KEMP, Simon, 2020. Digital 2020: 3.8 billion people use social media. En: *We Are Social* [en línea]. Disponible en: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media [Consulta: mayo 2020].

Linguee. *Diccionario inglés-español* [en línea]. Año 2020. Disponible en: https://www.linguee.es/ [Consulta: mayo 2020].

Real Academia Española. *Diccionario de la lengua española, 23.ª ed.* [en línea]. Diciembre de 2019. Disponible en: https://dle.rae.es/ [Consulta: mayo 2020]

RODRÍGUEZ, Xema, 2017. Machine Learning y Deep Learning: cómo entender las claves del presente y futuro de la inteligencia artificial. En: *Xataka* [en línea]. Disponible en: https://www.xataka.com/robotica-e-ia/machine-learning-y-deep-learning-como-entender-las-claves-del-presente-y-futuro-de-la-inteligencia-artificial [Consulta: mayo 2020].

SCHNEIER, Bruce, 2018. *Haz clic aquí para matarlos a todos. Un manual de supervivencia*. Barcelona: Editorial Planeta, 2019. ISBN 9788499987538.

UNIÓN EUROPEA. 1995. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea,* 23 de octubre de 1995 L 281/31. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES [Consulta: mayo 2020].

UNIÓN EUROPEA. 2016. 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 (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 4 de mayo de 2016 L 119/1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Consulta: mayo 2020].

8. Glosario

Amenaza [10]: «cualquier factor con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento» (AEPD Guía práctica de análisis de riesgos).

Autoridad de control [12]: «la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51; 4.5.2016 L 119/34 Diario Oficial de la Unión Europea ES» (art. 4.21 del RGPD).

Big Data [2]: «se emplea en el sector de las tecnologías de la información y de la comunicación para aludir a un conjunto de datos que, por su volumen y variedad y por la velocidad a la que necesitan ser procesados, supera las capacidades de los sistemas informáticos habituales» (Fundeu 2013).

Consentimiento del interesado [6]: «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen» (art. 4.11 del RGPD).

Datos biométricos [15]: «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos» (art. 4.14 del RGPD).

Datos genéticos [16]: «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona» (art. 4.13 del RGPD).

Datos personales [1]: «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» (art. 4.1 del RGPD).

Datos relativos a la salud [14]: «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud» (art. 4.15 del RGPD).

Deep Learning [5]: «es un subconjunto dentro del campo del Machine Learning, el cual predica con la idea del aprendizaje desde el ejemplo. En Deep Learning, en lugar de enseñarle a ordenador una lista enorme de reglas para solventar un problema, le damos un modelo que pueda evaluar ejemplos y una pequeña colección de instrucciones para modificar el modelo cuando se produzcan errores. Con el tiempo esperamos que esos modelos sean capaces de solucionar el problema de forma extremadamente precisa, gracias a que el sistema es capaz de extraer patrones» (Rodríguez 2017).

Destinatario [22]: «la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que 4.5.2016 L 119/33 Diario Oficial de la Unión Europea ES puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento» (art. 4.9 del RGPD).

Elaboración de perfiles [19]: «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física» (art. 4.4 del RGPD).

Encargado del tratamiento o Encargado [20]: «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento» (art. 4.8 del RGPD).

Fichero [17]: «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica» (art. 4.6 del RGPD).

Ingeniería social [23]: «La ingeniería social basa su comportamiento en una premisa básica: es más fácil manejar a las personas que a las máquinas. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente» (INCIBE 2019).

Inteligencia artificial [3]: «Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico» (RAE 2019).

Machine Learning [4]: «es la práctica de usar algoritmos para tratar datos, aprender de ellos y luego ser capaces de hacer una predicción o sugerencia sobre algo. Los programadores deben perfeccionar algoritmos que especifiquen un conjunto de variables para ser lo más precisos posibles en una tarea en concreto. La máquina es entrenada utilizando una gran cantidad de datos dando la oportunidad a los algoritmos a ser perfeccionados» (Rodríguez 2017).

Representante [21]: «persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento» (art. 4.17 del RGPD).

Responsable del tratamiento o Responsable [7]: «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros» (art. 4.7 del RGPD).

Riesgo [11]: «la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas» (AEPD guía práctica de análisis de riesgos).

Startup [9]: «una empresa emergente, normalmente con un alto componente tecnológico, con grandes posibilidades de crecimiento y que, por lo general, respalda una idea innovadora que sobresale de la línea general del mercado» (BBVA[42]).

Tercero [18]: «persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado» (art. 4.10 del RGPD).

Tratamiento [8]: «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

[42] Definición de startup: https://www.bbva.com/es/que-es-una-startup/

por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2 del RGPD).

Violación de la seguridad de los datos personales [13]: «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 4.12 del RGPD).

Anexos

I. Plantilla para el registro de actividades de tratamiento

Responsable del tratamiento

Nombre y datos de contacto

Delegado de Protección de Datos (si procede)

Nombre y datos de contacto

Descripción de la actividad de tratamiento y de los datos tratados

Actividad de tratamiento	Descripción de la actividad de tratamiento
Finalidad	Fines explícitos y la base jurídica
Interesados	Listado de personas físicas afectadas por la actividad de tratamiento: - Empleado - Cliente - Proveedor
Categorías de datos personales	Detalle del tipo de dato tratado: - Identificativo - Financiero - Profesional - Salud - Ideológico

Transferencias y cesiones

Cesiones	Identificar las categorías de los destinatarios de las cesiones previstas
Transferencias de datos internacionales	Descripción de las transferencias internacionales de los datos. Identificar al tercer país u organización, junto a la base jurídica que legitime el tratamiento
Periodo de conservación	Plazo previsto de conservación de la información

Medidas de seguridad

Medidas de seguridad	Descripción de las medidas técnicas y organizativas implantadas

Encargado del tratamiento

Nombre y datos de contacto

Delegado de Protección de Datos (si procede)

Nombre y datos de contacto

Descripción del tratamiento y de los datos tratados

Responsable del tratamiento	Nombre y datos de contacto del responsable que le ha encargado el tratamiento
Categorías de Tratamiento	Operaciones que conlleven la recogida, consulta, grabación, modificación, cesión o destrucción de datos personales por cada uno de los responsables a los que se preste el servicio

Transferencias y cesiones

Transferencias de datos internacionales	Descripción de las transferencias internacionales de los datos. Identificar al tercer país u organización, junto a la base jurídica que legitime el tratamiento

Medidas de seguridad

Medidas de seguridad	Descripción de las medidas técnicas y organizativas implantadas

II. Formulario para la realización de una EIPD

Una evaluación de impacto sobre la protección de datos (EIPD) es un procedimiento que busca identificar y controlar los riesgos para los derechos y libertades de las personas resultantes de un procesamiento de datos personales.

ANALIZAR LA NECESIDAD DE LA EIPD

Se requiere una descripción del tratamiento para determinar si es necesaria una EIPD. Esta descripción debe tener un nivel de detalle que le permita evaluar los supuestos e indicadores de riesgo detallados a continuación.

Descripción del tratamiento:

No es necesario hacer una EIPD si aplica cualquiera de los siguientes casos:

Supuesto	**¿Aplica?**
El tratamiento tiene naturaleza, alcance, contexto y finalidad similares a otro tratamiento para el que ya se ha realizado una EIPD.	
El tratamiento tiene una base jurídica en el Derecho de la UE o en un Estado miembro, y una EIPD ya se ha llevado a cabo en el momento de adoptar **esta** base jurídica.	
Justificación:	

Si no aplica ninguno de los casos anteriores, se debe realizar una EIPD si el tratamiento puede suponer un grave riesgo para los derechos y libertades de las personas. El Grupo de Trabajo del Artículo 29 (GT29) creado por la Directiva 95/46/CE, ofrece la siguiente lista de características que pueden ser indicativas de alto riesgo.

Indicador de riesgo potencial alto	**¿Aplica?**
Evaluación o puntuación, incluidas la elaboración de perfiles y predicciones.	
Toma de decisiones automatizada con efectos legales o que afecta al individuo de una manera similar y significativa.	
Observación sistemática de un área de acceso público.	
Datos sensibles	
Tratamiento de datos a gran escala	
Conjuntos de datos que se han vinculado o combinado.	
Datos relacionados con personas vulnerables	
Uso innovador de tecnologías.	
Tratamiento que en sí mismo impide el ejercicio de un derecho o el uso de un servicio o contrato	

Según el GT29, es necesario hacer una EIPD cuando el tratamiento presenta dos o más casos de la tabla, aunque indica que puede ser conveniente hacer la EIPD incluso en algunos casos donde sólo aplica uno. Si hay dos más y se considera que una EIPD no es necesario, hay que justificarlo.

¿Es necesario hacer la EIPD? ¿Por qué?

Si se ha nombrado un DPD, es necesario considerar su opinión con respecto a la necesidad de hacer una EIPD.

Opinión del DPD:

DESCRIPCIÓN DEL CICLO DE VIDA DE LOS DATOS

Es necesario hacer una descripción del tratamiento lo más detallada posible, ya que esta será la base para evaluar la necesidad, la proporcionalidad y los riesgos del tratamiento.

Descripción detallada del tratamiento:

Finalidad del tratamiento:

Datos personales procesados

Las características de los datos a tratar son relevantes a la hora de determinar los riesgos del tratamiento y el cumplimiento de algunas disposiciones de la normativa.

(Rellenar una tabla por tipo de datos)

Tipo de datos	
Fuente	
Período de conservación	
¿Datos especialmente sensibles?	
¿Usar para otro propósito que no sea la colección?	

Actores involucrados en el tratamiento

Los actores involucrados en el tratamiento, su función y los datos que procesan son importantes a la hora de determinar los riesgos del tratamiento.

(Rellenar una tabla por tipo de datos)

Nombre	
Procesos en los que interviene	
Descripción	

Procesos del tratamiento

El objetivo de esta sección es dividir el tratamiento en partes más pequeñas para que sean más coherentes y fáciles de explicar.

(Rellenar una tabla por cada etapa del procesamiento)

Proceso	
Descripción	
Datos procesados	
Resultado del proceso	
Destinatario	
Lugar del tratamiento	

Transferencias de datos

Compartir datos con agentes externos puede aumentar los riesgos del tratamiento; especialmente si se realizan en terceros países donde el RGPD no se aplica.

¿Se comparten los datos? Describe qué datos se comparten, el destinatario y el motivo.

ANÁLISIS DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

La evaluación de la necesidad y la proporcionalidad del tratamiento se lleva a cabo en relación con la finalidad de este, descrita en la sección anterior.

Finalidad del tratamiento

En principio, los datos recogidos se utilizan para lograr el propósito del tratamiento que motivó la recolección. Sin embargo, en algunos casos, el Reglamento permite el tratamiento de datos que han sido recogidos para un propósito diferente.

¿Se recopilan datos para un fin distinto al de este tratamiento?	Sí / No

Si es así,

Las siguientes condiciones permiten el tratamiento de los datos para un fin distinto al de la recogida.

El consentimiento de los interesados en el tratamiento se ha obtenido para la nueva finalidad.	
El tratamiento se basa en el derecho de la unión o de los Estados miembros que constituye una medida para salvaguardar:	
• la seguridad nacional	
• la defensa	
• la seguridad pública	
• prevención, investigación, detección y tramitación de delitos	
• otros objetivos importantes de interés público	
• la protección de la independencia y los procedimientos judiciales	
• la prevención, investigación, detección y procesamiento de violaciones en las normas deontológicas	
• la protección de la parte interesada o de los derechos y libertades de otros	
• la ejecución de demandas civiles	

Si no se aplica ninguna de las condiciones anteriores, la nueva finalidad debe ser compatible con la finalidad que condujo a la recogida de los datos

Propósito inicial	
Datos	
Nuevo propósito	
Justificación de la compatibilidad	

Principios de licitud y lealtad

Base legal para el tratamiento

Un tratamiento es lícito si aplica alguna de las bases legales siguientes:

El interesado ha dado su consentimiento para el tratamiento de sus datos personales, para uno o más fines específicos.	
El tratamiento es necesario para ejecutar un contrato en el que el interesado forma parte de este o para aplicar medidas precontractuales.	
El tratamiento es necesario para cumplir con una obligación legal aplicable al responsable del tratamiento.	
El tratamiento es necesario para proteger los intereses vitales del interesado u otra persona física.	
El tratamiento es necesario para cumplir una misión realizada en interés público o en el ejercicio de los poderes públicos conferidos al responsable del tratamiento.	
El tratamiento es necesario para satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, siempre que no prevalezcan los intereses o derechos y libertades fundamentales del interesado (en particular, cuando el interesado sea menor de edad).	
Justificación de la legalidad del tratamiento	

Además, el tratamiento no debe incurrir de manera ilícita en un sentido más amplio. Por ejemplo, violar los derechos de autor o acuerdos contractuales.

Confirma que el tratamiento no incurre en ningún tipo de ilícito.

Tratamiento de datos de menores

Los menores necesitan una protección especial en el tratamiento de sus datos, ya que pueden no ser conscientes de los riesgos involucrados.

¿Ofrece el tratamiento servicios de la sociedad de la información a los niños y tiene como base el consentimiento?	Sí / No
En caso afirmativo, ¿se ha tenido en cuenta la edad mínima de consentimiento?	Sí / No

Tratamiento de categorías especiales de datos

¿Son datos de categorías especiales?	Sí / No

Si es así,

El procesamiento de categorías especiales de datos está prohibido, a menos que aplique cualquiera de los siguientes casos.

El interesado ha dado su consentimiento explícito para el tratamiento para un fin específico, a menos que la legislación de la UE o de los estados miembros no lo permita.	
El tratamiento es necesario para cumplir las obligaciones o para ejercer derechos en el ámbito del derecho laboral y de la seguridad y la protección social.	
El tratamiento es necesario para proteger los intereses vitales del interesado u otra persona, y el interesado no está capacitado para dar su consentimiento.	
El tratamiento es necesario para proteger los intereses vitales del interesado u otra persona física.	
El tratamiento es legítimo y con garantías, realizadas por una asociación sin ánimo de lucro de carácter político, filosófico, religioso o sindical, siempre que el tratamiento afecte a las personas con las que mantienen contactos en relación con estos fines y los datos no se comuniquen a terceros sin el consentimiento de los interesados.	
El tratamiento se refiere a los datos que el interesado ha hecho públicos.	
El tratamiento es necesario para formular, ejercer o defender reclamaciones, o cuando los tribunales actúen en su función judicial.	
El tratamiento es necesario por razones de interés público esencial.	

El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad de trabajo del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.	
El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.	
El tratamiento es necesario para fines de archivo con interés público, investigación científica o histórica, o con fines estadísticos.	
Justificación de la legalidad del tratamiento de datos en categorías especiales.	

Tratamiento de datos penales

¿Se procesan datos relacionados con condenas o delitos penales?	Sí / No

Si es así,

Aunque los datos relativos a condenas o infracciones penales no son categorías especiales de datos, existe un requisito adicional para procesarlos: el tratamiento sólo puede llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el derecho de la unión o del estado miembro.

Justificación de la legalidad del tratamiento de datos penales.

Validez del consentimiento

Si un tratamiento tiene como base jurídica el consentimiento, deben cumplirse las siguientes condiciones para que sea válido:

El responsable debe ser capaz de demostrar que lo ha recogido.	
La solicitud de consentimiento es inteligible, de fácil acceso y en un lenguaje claro.	
La ejecución de un contrato no puede ser utilizada para recibir el consentimiento con respecto a los datos personales no necesarios para ejecutar el contrato.	
Los interesados han sido informados de la posibilidad de retirar el consentimiento en cualquier momento.	

Transferencias de datos

Para evitar que los interesados vean reducidos sus derechos, el RGPD es especialmente restrictivo con transferencias de datos con países donde el RGPD no se aplica.

¿Se realizan transferencias a terceros países u organizaciones internacionales?	Sí / No

Si es así,

Estas transferencias están permitidas si la Comisión Europea considera que el país u organización ofrece un nivel adecuado de protección, si se han establecido garantías suficientes de conformidad con el artículo 46 o si se ha establecido alguna de las excepciones del artículo 49.

(Rellenar una tabla por cada transferencia)

Datos transferidos	
País	
Condición que permite la transferencia	

Lealtad del tratamiento

Un tratamiento es leal si hace el uso de los datos previsibles por parte de las partes interesadas, y el tratamiento no da lugar a consecuencias adversas para las partes interesadas que no sean justificables.

Justificación del trato leal

Principio de minimización

Los datos deben ser adecuados, relevantes y limitados a lo estrictamente necesario para cumplir con la finalidad del tratamiento.

(Rellenar una tabla por tipo de datos)

Tipos de datos	
Justificación de la adecuación, pertinencia y necesidad	

Principio de limitación del período de conservación

Los datos personales no deben conservarse más tiempo del estrictamente necesario para cumplir con la finalidad del tratamiento. En la descripción del procesamiento, se especificó el período de retención de datos. Es necesario justificar que los plazos dados cumplen el principio de limitación del período de conservación.

Justificación de que los plazos de conservación dados cumplen con la limitación del período de conservación.

Es necesario que los mecanismos establecidos para eliminar los datos sean eficaces. (¿Es automático o debe realizarse manualmente? ¿Los datos permanecen en las copias de seguridad del sistema una vez eliminados? ¿Cuánto tiempo y cómo se garantiza que no se procesarán? etc.).

Describe los mecanismos establecidos para borrar datos.

Los datos pueden conservarse indefinidamente para fines de archivo de interés público, con fines de investigación científica o histórica, o con fines estadísticos.

Los datos se conservan para los fines del archivo de interés público, con fines de investigación científica o histórica, o con fines estadísticos.	
En caso afirmativo, ¿qué medidas se han aplicado para garantizar el principio de minimización?	

Principio de exactitud

El tratamiento de datos inexactos puede afectar negativamente a las personas. El principio de exactitud exige que los datos sean precisos y que se tomen las medidas adecuadas para garantizar que los inexactos se actualicen o eliminen sin demora.

Controles de calidad de los datos

Medidas para corregir datos

Necesidad y proporcionalidad del tratamiento

Con la información recogida en esta sección, es necesario justificar que el tratamiento es necesario (el propósito buscado no puede ser abordado con cualquier otra medida más moderada) y proporcional (no causa más daño que beneficios).

Justificación de la eficacia del tratamiento para el propósito que busca.

Justificación de la necesidad de tratamiento.

Justificación de que el tratamiento es proporcional

Opinión de las partes interesadas

El RGPD establece que, si es posible, se debe recoger la opinión de los interesados sobre el tratamiento.

Opinión de los interesados en la necesidad y proporcionalidad del tratamiento.

Si no se considera apropiado recoger la opinión de los interesados, es necesario justificarlo.

¿Por qué no se ha recogido la opinión de los interesados?

Si la opinión de los interesados respecto al tratamiento difiere de la visión que el responsable ha proporcionado anteriormente y se pretende continuar con el tratamiento, se debe justificar.

¿Por qué se lleva a cabo el tratamiento a pesar de las discrepancias de los interesados?

GESTIÓN DE RIESGOS

El objetivo de este punto es identificar los posibles efectos negativos sobre las personas, cuantificarlos y si es necesario proponer medidas para mitigarlos.

En un primer momento evaluaremos el tratamiento tal y como está diseñado. Es decir, no tenemos en cuenta los casos en los que se produce un error en la seguridad del sistema (ya sea un error accidental o intencionado).

Para identificar los posibles efectos negativos del tratamiento en las personas es aconsejable tener en cuenta el punto de vista de los interesados y del delegado de protección de datos.

Posibles efectos negativos del tratamiento en las personas

Para cada uno de los efectos negativos identificados, es necesario estimar el nivel de riesgo asociado. El riesgo depende de dos factores: el impacto que tiene sobre las personas (despreciable, limitado, significativo o máximo) y la probabilidad de que se materialice (despreciable, limitada, significativa o máxima). El impacto se estima directamente de los efectos potenciales. Para determinar la probabilidad, es necesario

analizar qué circunstancias hacen que los efectos negativos se materialicen (las amenazas) y estimar la probabilidad de ellos.

El riesgo se determina, dependiendo del impacto y la probabilidad, siguiendo la siguiente matriz de riesgos:

Probabilidad					
	Máxima	Riesgo medio	Riesgo alto	Riesgo muy alto	Riesgo muy alto
	Significativa	Riesgo medio	Riesgo medio	Riesgo alto	Riesgo muy alto
	Limitada	Riesgo bajo	Riesgo medio	Riesgo medio	Riesgo alto
	Despreciable	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo medio
		Despreciable	Limitado	Significativo	Máximo
		Impacto			

En primer lugar, se estimará el riesgo asociado a cada amenaza. El riesgo global será el máximo de los riesgos de las amenazas.

Efecto en las personas:

Impacto:

Amenaza	Probabilidad	Riesgo

Riesgo estimado:

A menos que el riesgo sea bajo, se deben buscar medidas para reducirlo. Esto es especialmente necesario en casos de riesgo alto o muy alto. Si no es posible reducir un riesgo alto, antes de empezar el tratamiento hay que consultar a la autoridad de protección de datos sobre su idoneidad.

Si el tratamiento inicial ha sido alterado para que sea menos lesivo para las personas, las secciones anteriores de la EIPD deberán ser revisadas y actualizadas.

Medidas para garantizar los derechos de los interesados

Controles del derecho a tener información transparente

La transparencia es transversal y debe estar presente en todas las comunicaciones con los interesados.

Toda comunicación con los interesados debe ser concisa, inteligible, de fácil acceso y debe hacer uso de un lenguaje claro y sencillo.	

El reglamento regula la forma como se debe hacer esta comunicación

La información se facilitará por escrito (incluidos los medios electrónicos).	
En el caso de solicitudes realizadas con medios electrónicos, la información será preferiblemente electrónica.	
Si el interesado lo solicita, la información se facilitará oralmente.	

El responsable del tratamiento deberá responder a las solicitudes de ejercicio de los derechos de los interesados dentro de los plazos establecidos:

Sin demoras indebidas y no más de un mes.	
Si la complejidad o el número de solicitudes lo justifica, el período puede ampliarse por dos meses. En este caso es necesario informar los motivos dentro del primer mes.	

Si el responsable del tratamiento no tiene que responder a la solicitud de ejercicio de los derechos de un interesado, es necesario:

Notificar al interesado de este hecho sin demora indebida y como máximo en un mes.	
Explicar las razones para no llevar a cabo la solicitud (por ejemplo, la solicitud es repetitiva o la persona responsable no puede identificar al interesado).	
Informe sobre la posibilidad de apelar la decisión ante una autoridad de control o un juzgado	

Sólo si la solicitud es excesiva (por ejemplo, repetitiva), se puede cobrar un cargo para cubrir los costes de procesamiento de esta.	

Controles para el derecho de información

Al recopilar datos personales, el responsable del tratamiento deberá informar a los interesados de los diferentes aspectos del tratamiento.

Los artículos 13 y 14 especifican que es necesario informar a los interesados de los puntos de la tabla siguiente:

La identidad y los datos de contacto del responsable	
Los datos de contacto del delegado de protección de datos (si lo hubiera)	
La finalidad del tratamiento	
La base jurídica del tratamiento	
El interés legítimo del responsable, si esta es la base jurídica del tratamiento	
Destinatarios o categorías de destinatarios de datos	
El período de conservación de los datos o el criterio utilizado para determinarlo	
La intención de transmitir los datos fuera de la UE (si procede)	
La decisión de la Comisión Europea sobre la suficiencia de seguridad ofrecida por el país u organización de destino	
La existencia del derecho de acceso a los datos	
La existencia del derecho de rectificación y supresión	
La existencia del derecho a limitar el tratamiento	
La existencia del derecho de oposición al tratamiento	
La existencia del derecho de portabilidad de los datos	

La existencia del derecho a revocar el consentimiento (si esta es la base jurídica del tratamiento)	
La existencia del derecho a presentar una queja ante una autoridad de control	
Que la comunicación de los datos es un requisito legal o contractual, en su caso	
La existencia de decisiones automatizadas	
El propósito de utilizar los datos para un fin distinto al que motivó a la recogida (si procede)	
El origen de los datos, si no se han obtenido directamente del interesado	

Existen algunas exenciones a la obligación de informar que dependen de la forma en que se recopilaron los datos.

- Si los datos han sido obtenidos directamente del interesado, no hay obligación de informarle si ya dispone de la información.
- Si los datos no se han obtenido directamente del interesado, no es necesario informarle si se da alguna de las siguientes condiciones[43]: el interesado ya dispone de esta información, la comunicación es imposible o representa un esfuerzo desproporcionado, así esté regulada por una norma de la UE o de los estados miembros o la información es confidencial sobre la base del secreto profesional.

Si no se informa, debe justificarse.

¿Se aplica el derecho de información a todos los datos procesados?	
Si se aplica alguna exención al derecho de información, es necesario decir cuál, a qué datos y justificar el motivo.	

Si se informa a los interesados, el RGPD determina cuándo hacerlo[44].

Si los datos se recogen directamente de los interesados, en el momento de su recogida.	
Si los datos se recopilan indirectamente, deben cumplirse las siguientes condiciones:	
• En un período de tiempo razonable y no superior a un mes.	
• Si nos comunicamos con los interesados, no más tarde del momento de la primera comunicación.	
• Si desea comunicar los datos a terceros, antes de comunicarlos.	

Controles para garantizar el derecho de acceso

El interesado tiene derecho a obtener del responsable del tratamiento la confirmación de que sus datos están siendo tratados y, en este caso, el derecho de acceso a los datos personales y la siguiente información:

La finalidad del tratamiento	

[43] RGPD art. 14.5
[44] RGPD art 13.1 y art 14.3

Las categorías de datos tratados	
Los destinatarios de los datos	
El período de retención de datos	
Los derechos para rectificar y eliminar los datos	
El derecho a limitar y oponerse al tratamiento	
El derecho a reclamar ante una autoridad de control	
Si los datos no se han obtenido del interesado, el origen de estos	
La existencia de decisiones automatizadas (si procede)	
Garantías en la transferencia de datos fuera de la UE (si procede)	

Además de saber qué información debe transmitirse a los interesados, es necesario garantizar que se dan las condiciones para hacer valer el derecho de acceso.

¿Se ha establecido un procedimiento estándar para gestionar las solicitudes de acceso?	
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de acceso?	

Controles para garantizar el derecho de rectificación

Las personas tienen derecho a rectificar sus datos, si estos no son exactos.

¿Se ha establecido un procedimiento para gestionar las solicitudes de rectificación?	
¿El personal que trata con las personas interesadas tiene la formación necesaria para reconocer las solicitudes de rectificación?	

Si el responsable del tratamiento ha compartido los datos, debe informar a los destinatarios sobre la rectificación.

¿Se ha establecido un procedimiento para notificar a los destinatarios de la rectificación?	

Derecho de supresión

Las personas tienen derecho a eliminar su información cuando se da cualquiera de los siguientes casos:

- Los datos ya no son necesarios en relación con la finalidad por la que se recopilaron.
- El interesado retira su consentimiento y no hay ninguna otra base legal para el tratamiento.
- El interesado se opone al tratamiento y no hay otro factor superior que lo legitime.
- Los datos han sido tratados sin base jurídica.
- Los datos deben ser eliminados de acuerdo con una obligación legal que afecta al responsable.
- Los datos se utilizan para proporcionar servicios de la sociedad de la información a los niños.

Sin embargo, el derecho de supresión no se aplica en los siguientes casos:

- Ejercer el derecho a la libertad de expresión e información.
- Cumplir con una obligación legal o de interés público.
- A los efectos de la presentación de un interés público, con fines de investigación científica o histórica, y con fines estadísticos (si el cumplimiento de estos fines se vio afectado por la supresión de datos).
- Para presentar, ejercer o defender reclamaciones legales.

¿Tiene el personal la capacidad de decidir si aplica el derecho a la supresión?	

Es aconsejable establecer un canal estándar para que los interesados puedan solicitar hacer efectivo el derecho de supresión. Sin embargo, es necesario garantizar que el personal esté capacitado para detectar solicitudes realizadas por otros medios.

¿Se ha establecido un procedimiento para administrar las solicitudes de supresión?	
¿Tiene el personal que se ocupa de tratar con los interesados la formación necesaria para reconocer las solicitudes de supresión?	

Si el controlador de datos comparte los datos, debe tomar las medidas adecuadas (teniendo en cuenta los costos y la tecnología disponibles) para notificar a los destinatarios sobre la solicitud de eliminación.

¿Se ha establecido un procedimiento para notificar la solicitud de supresión a los destinatarios?	

Derecho a limitar el tratamiento

El artículo 18 otorga a las personas el derecho a limitar el tratamiento de sus datos, en los siguientes casos:

- El interesado ha solicitado la rectificación de sus datos y el responsable del tratamiento está verificando si son exactos.
- Los datos han sido tratados sin base jurídica.
- El interesado necesita que el responsable guarde los datos para iniciar, ejercer o defender una reclamación.
- El interesado se ha opuesto al tratamiento y el responsable está evaluando si los motivos legítimos del responsable prevalecen sobre los del interesado.

¿Está capacitado el personal para decidir si se aplica el derecho a limitar el tratamiento?	

Es necesario asegurarse de que el personal está capacitado para detectar solicitudes de limitación de tratamiento.

¿Se ha establecido un procedimiento para la gestión de las solicitudes de limitación del tratamiento?	
¿El personal que se ocupa de tratar con los interesados tiene la formación necesaria para reconocer las solicitudes de limitación del tratamiento?	

Al limitar el tratamiento, hay que tener en cuenta las diferentes formas que este puede tener: recopilación de datos, análisis de datos, difusión de resultados, etc.

¿Se tienen en cuenta todas las posibles formas de tratamiento a la hora de limitarlo?	

Si se han compartido datos, se debe informar a los destinatarios sobre las solicitudes de limitación del tratamiento.

¿Se ha establecido un procedimiento para notificar la solicitud de limitación del tratamiento a los destinatarios?	

Derecho a la portabilidad de los datos

Las personas tienen derecho a solicitar los datos que han proporcionado al responsable del tratamiento en los siguientes casos:

- Si el tratamiento se basa en el consentimiento, o es necesario para ejecutar un contrato o para aplicar medidas precontractuales.
- El tratamiento se realiza con medios automatizados.

El derecho a la portabilidad de los datos no se limita a los datos que las personas han proporcionado explícitamente; también afecta a los datos recopilados de la observación de las personas.

¿Está capacitado el personal para decidir si se aplica el derecho a la portabilidad de los datos?	

El derecho a la portabilidad de los datos no debe afectar negativamente a otras personas. En particular:

- Si los datos personales contienen información de un tercero, es necesario evaluar si este puede verse afectado por sus derechos y libertades.
- Si los datos están asociados con varias personas (por ejemplo, una cuenta bancaria compartida), debe buscar el consenso de todos los interesados.

¿Tiene en cuenta el procedimiento para efectuar el derecho a la portabilidad de los datos, el efecto sobre los derechos y libertades de otras personas?	

Es necesario asegurarse de que el personal está capacitado para detectar solicitudes de portabilidad de datos.

¿Se ha establecido un procedimiento para la gestión de solicitudes de portabilidad de datos?	
¿El personal que se ocupa de tratar con los interesados tiene la formación necesaria para reconocer las solicitudes de portabilidad de datos?	

El RGPD determina cómo debe llevarse a cabo la portabilidad.

¿Se utiliza un formato estructurado, de uso común y que sea de fácil lectura?	

Derecho de oposición

Las personas tienen derecho a oponerse al tratamiento de su información cuando dicho tratamiento se realice sobre la base de:

- El interés público o el ejercicio de los poderes públicos conferidos al responsable del tratamiento.
- El interés legítimo del responsable del tratamiento.

En este caso, el responsable debe acabar con el tratamiento, a menos que certifique motivos legítimos que prevalezcan sobre los derechos del interesado.

¿Está capacitado el personal para decidir si aplica el derecho a la oposición?	

Tenemos que asegurarnos de que el personal esté capacitado para detectar solicitudes de oposición.

¿Se ha establecido un procedimiento para gestionar las solicitudes de oposición al tratamiento?	
¿El personal que se ocupa de tratar con los interesados tiene la formación necesaria para reconocer las solicitudes de oposición al tratamiento?	

El RGPD especifica cómo actuar al recibir una solicitud de oposición al tratamiento en varios casos.

Si la solicitud se opone al procesamiento con fines de marketing, debe aceptarse sin excepción.	
Si la solicitud se opone al tratamiento con fines de investigación científica o histórica, o con fines estadísticos, debe aceptarse a menos que el tratamiento se realice en interés público.	

Derecho a no estar sujeto a decisiones automatizadas

¿El tratamiento automatizado tiene efectos legales u otros efectos significativos en las personas?	Sí / No
Si es así, ¿qué base jurídica lo permite?	
• Es necesario para la ejecución de un contrato entre el interesado y el responsable	
• Está autorizado por el derecho de la unión o de un estado miembro	
• El interesado ha dado su consentimiento explícito	

El interesado siempre tiene derecho a obtener una intervención humana, a expresar su punto de vista y a impugnar la decisión.

¿Existe un procedimiento para que las personas soliciten la intervención humana, expresen su punto de vista y impugnen la decisión?	
¿Hay personal en la organización con la capacidad de revisar las decisiones y cambiarlas?	

Las decisiones automatizadas sólo pueden utilizar categorías especiales de datos si existe el consentimiento explícito del interesado, o si el tratamiento se realiza para proteger los intereses vitales del interesado u otra persona.

¿Se hace uso de categorías especiales de datos en el tratamiento automático?	Sí / No
Si es así, ¿qué base jurídica lo permite?	
• El interesado ha dado su consentimiento explícito	

• El tratamiento se realiza para proteger los intereses vitales del interesado u otra persona	

Riesgos en la seguridad de los datos

Según el RGPD, las medidas utilizadas para proteger la información deben ser adecuadas al riesgo para los derechos y libertades de las personas. En esta sección seguimos una metodología sencilla para analizar los riesgos relacionados con la seguridad de los datos. Es decir, los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de datos.

Impacto

Evaluamos el impacto que la pérdida de confidencialidad, integridad y disponibilidad de datos personales tiene sobre el interesado.

Para fijar el impacto sobre las personas de la pérdida de seguridad de los datos, es necesario tener en cuenta las características del tratamiento. Entre otras:

- El tratamiento de datos de categorías especiales u otros datos especialmente sensibles (información financiera, ubicaciones, etc.).
- Monitorización de personas.
- El tratamiento de datos de grupos con necesidades especiales (menores, autoridades, etc.).
- El tratamiento de grandes cantidades de datos de cada persona.

Con el fin de contextualizar el cálculo del impacto, se proponen diferentes escenarios en los que se pierde alguna de estas propiedades.

Impacto que la pérdida de confidencialidad de los datos (es decir, del acceso no autorizado a los datos) tiene sobre las personas. Ejemplos de casos de pérdida de confidencialidad: • Pérdida o robo de un ordenador que contenga datos personales. • Envío de datos personales a personas no autorizadas por error. • Posibilidad de acceso no autorizado a la cuenta de una persona. • Un error de configuración en un sitio web expone los datos personales de sus usuarios. • Robo de información de las instalaciones del responsable o del encargado del tratamiento. • Un empleado de un centro médico consulta de manera no autorizada el archivo de un paciente.
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

Impacto que la pérdida de la integridad de los datos (es decir, de la modificación no autorizada de los datos) tiene sobre las personas. Ejemplos de casos de pérdida de integridad: • Un empleado modifica erróneamente los datos de un cliente. • Un error en la red de comunicaciones altera los datos mientras están en tránsito. • Por razones operativas, una empresa mantiene varias copias de los datos, pero un cambio en una de las copias no se propaga a las demás. • Pérdida de parte de un archivo, como resultado de un fallo en el sistema de tratamiento.
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

Impacto que la pérdida de disponibilidad de datos tiene sobre las personas. Ejemplos de casos de pérdida de disponibilidad: • Un archivo está dañado o eliminado y no hay ninguna copia de seguridad. • Se pierde un archivo del que sólo había una copia impresa. • Un servicio de consulta de datos deja de estar disponible (por ejemplo, el servicio para tener acceso a registros de salud electrónicos).
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

El impacto del sistema será el máximo de los tres casos anteriores.

Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto

Probabilidad inicial

La siguiente tabla muestra las características del tratamiento que aumentan los riesgos de seguridad de los datos. Estimaremos la probabilidad de fallo de seguridad dependiendo del número de características que se cumplan.

Hardware y software	
P1. ¿El sistema de tratamiento está conectado a sistemas externos a la organización? La conexión con sistemas externos a la organización aumenta la exposición a las amenazas. Por ejemplo, la información se puede capturar o modificar de forma malintencionada mientras está en tránsito. Ejemplos: • El sistema de tratamiento de un hospital está conectado al sistema público de seguridad social y a los sistemas de las aseguradoras privadas. • Las estaciones de trabajo que forman parte del sistema de tratamiento tienen acceso a Internet.	☐Sí ☐No
P2. ¿Alguna parte del tratamiento se realiza a través de Internet? La interacción con los interesados a través de Internet expone el sistema de tratamiento a amenazas externas, *como phishing,* inyección SQL, ataques *man-in-the-middle,* DoS y XSS. Estas amenazas pueden poner en peligro el sistema del tratamiento y afectar a las propiedades de seguridad de los datos (confidencialidad, integridad y disponibilidad). Permitir a los trabajadores acceder al sistema de tratamiento a través de Internet también aumenta la exposición a ataques externos y también aumenta la posibilidad de que los trabajadores hagan un uso indebido de la información (accidental o intencional). Ejemplos: • Tienda online, banca online, etc. • El correo electrónico se utiliza en el tratamiento. • Los administradores del sistema del tratamiento pueden llevar a cabo tareas de mantenimiento o supervisión a través de Internet. El acceso al sistema de tratamiento desde un espacio público puede facilitar a las personas ajenas a la organización su observación	☐Sí ☐No

P3. ¿Falta de seguimiento de un documento de buenas prácticas relevante en el diseño o configuración del sistema de tratamiento? Si el sistema de tratamiento no está bien diseñado o los elementos que lo componen no están configurados correctamente, se incrementan los riesgos para la seguridad de los datos. Hay muchas guías de buenas prácticas en seguridad con diferentes temas (red, equipo, etc.). Ejemplos: • Debe diseñar la red siguiendo un documento de práctica recomendada que incluya elementos como firewalls, segmentación de red y uso de VPN. • Es necesario hacer uso de un documento de buenas prácticas, al configurar el sistema operativo. Esto implica medidas como el uso de antivirus y no permitir el uso de contraseñas inseguras. • Es necesario dimensionar el sistema de tratamiento pensando en las necesidades computacionales, de comunicación y de almacenamiento que se prevén. También es necesario proporcionar suficiente personal. • Es necesario hacer uso de un documento de buenas prácticas, al configurar el software. Por ejemplo, cómo configurar un servidor web para que sea más seguro. • Es necesario utilizar una metodología de desarrollo que tenga en cuenta la seguridad de los datos a lo largo del ciclo de vida de la aplicación.	☐Sí ☐No
P4. ¿Falta de seguimiento de un documento de buenas prácticas relevante en el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento? Es esencial mantener y supervisar adecuadamente el sistema. El mantenimiento debe realizarse tanto para dispositivos como para software. La supervisión del sistema no sólo nos permite analizar un incidente una vez que se ha producido, sino que también ayuda a detectar comportamientos sospechosos para evitar que el incidente ocurra, o para reducir su impacto. Ejemplos: • No aplicar las actualizaciones de seguridad del sistema operativo puede dar lugar a nuevos vectores de ataque. • La falta de copias de seguridad regulares puede llevar a la pérdida de información en caso de un incidente.	☐Sí ☐No

P5. ¿Hay falta de seguridad física en las instalaciones donde se lleva a cabo el tratamiento? La seguridad física de las instalaciones de tratamiento es esencial. Sin esto, no se puede garantizar la seguridad del sistema de tratamiento (ya sea electrónico o no). Ejemplos: • El CPD no está debidamente protegido con un sistema que impide el acceso a personas no autorizadas. • Las restricciones de espacio han hecho que parte del archivo de papel esté distribuido en diferentes áreas, que no garantizan su seguridad. • CPD no está protegido contra accidentes naturales e industriales (por ejemplo, fallas eléctricas, inundaciones). • Hace uso de un servicio en la nube sin tener garantías de que las instalaciones del proveedor están suficientemente protegidas.	☐Sí ☐No

Uso del sistema de tratamiento	
P6. ¿Hay falta de claridad en la definición de las funciones y responsabilidades de los trabajadores? La falta de claridad en la definición de las funciones y responsabilidades puede conducir a un uso incontrolado de los datos (ya sea accidental o intencional). Ejemplos: • Un trabajador de una sucursal bancaria solo debe comprobar los datos de sus clientes. • Los trabajadores son responsables de destruir la información (digital o no) de forma segura, cuando deja de ser necesaria. • Los trabajadores son responsables de mantener la seguridad de los datos cuando se los comunican a otra persona u organización.	☐Sí ☐No
P7. ¿Hay falta de claridad a la hora de definir los usos aceptables de los sistemas de tratamiento? Cuando no se definen claramente los usos aceptables de los sistemas de tratamiento, aumenta el riesgo de hacer un uso indebido y de introducción de vulnerabilidades en el sistema. Ejemplos: • La instalación de software de intercambio de archivos puede conducir a la compartición involuntaria de archivos. • La instalación de software por parte de usuarios que no son administradores puede provocar un mantenimiento deficiente. • Visitar páginas web maliciosas puede establecer una fuente de entrada de malware y robo de datos.	☐Sí ☐No

P8. ¿Puede el personal conectar dispositivos externos al sistema? La conexión de dispositivos externos al sistema de tratamiento es una puerta de entrada de malware, de introducción de vulnerabilidades, etc. Además, también facilita la extracción de información. Ejemplos: • El personal conecta el teléfono o una memoria USB a los puertos del ordenador. • El personal puede utilizar sus dispositivos para realizar tareas relacionadas con el tratamiento (BYOD).	☐Sí ☐No
P9. ¿Existe un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento? La falta de un archivo de registro de las actividades (fichero log) puede aumentar la mala praxis del personal y, al mismo tiempo, obstaculizar la investigación de los incidentes una vez que se han producido. Ejemplos: • Puede consultar los archivos de clientes / pacientes sin que quede registrado. • Aunque se genera un registro de actividades, no se supervisa. • No hay registro de personas que entran en CPD.	☐Sí ☐No

Personas involucradas en el tratamiento	
P10. ¿El personal recibe permisos que no son necesarios para cumplir con las tareas encomendadas? Cuanto mayor sea el número de personas que tienen acceso a los datos, mayor será la probabilidad de abuso. Para evitarlo, es esencial que el sistema controle el acceso al sistema del personal y autorice únicamente los accesos estrictamente necesarios para cumplir con las tareas encomendadas. Ejemplos: • El acceso a la historia clínica de un paciente debe limitarse a los profesionales que lo tratan.	☐Sí ☐No
P11. ¿Alguna parte del tratamiento ha sido subcontratada a un encargado? La externalización del tratamiento o parte del tratamiento a un encargado representa una pérdida de control sobre los datos. Es necesario elegir un encargado que pueda ofrecer un alto nivel de seguridad y definir claramente sus responsabilidades. Ejemplos: • Una nube se utiliza para realizar parte del tratamiento. • Se contratan servicios especializados para analizar algunos datos.	☐Sí ☐No

P12. ¿Existe un desconocimiento del personal sobre el uso adecuado del sistema, de los aspectos de la seguridad de los datos o de las limitaciones de uso impuestas por el RGPD? La falta de conocimiento sobre el uso esperado del sistema, sobre la seguridad de la información o sobre las obligaciones y limitaciones impuestas por el RGPD puede conducir a malas prácticas. Ejemplos: • La falta de conocimiento de seguridad puede hacer que el personal que se ocupa de los datos sea más probable que siga las instrucciones de un correo electrónico de *phishing.* • El personal debe recordar la necesidad de guardar documentos físicos en las condiciones de seguridad adecuadas.	☐Sí ☐No

Otras características	
P13. ¿Ha sufrido la empresa u otras empresas del sector ataques últimamente? La existencia de ataques anteriores debe tomarse como una advertencia de posibles ataques futuros. Es aconsejable tomar las medidas necesarias para evitar que ataques similares tengan éxito.	☐Sí ☐No
P14. ¿Se han recibido quejas de alguien sobre la estabilidad o seguridad del sistema de tratamiento últimamente? La presencia de errores en el sistema de tratamiento aumenta la probabilidad de sufrir un ataque. Del mismo modo, las advertencias sobre posibles errores de seguridad del sistema también pueden indicar una mayor probabilidad de sufrir ataques. Ejemplos: • Cuando se introducen datos incorrectos en un formulario, la aplicación de procesamiento muestra un error y finaliza inesperadamente. • Se ha notificado a un usuario que el sistema es vulnerable a un ataque específico.	☐Sí ☐No
P15. ¿Se tratan datos de especial interés o datos de un gran número de usuarios? La presencia masiva de datos y la presencia de datos de especial interés son una motivación adicional para los atacantes potenciales. Ejemplo: • Una gran empresa que almacena datos personales y financieros de sus clientes (por ejemplo, número de tarjeta de crédito).	☐Sí ☐No

Calculamos la probabilidad inicial de basarse en el número de respuestas afirmativas de acuerdo con la siguiente tabla:

Respuestas afirmativas	Probabilidad inicial
0 - 4	Bajo
5 – 9	Promedio
10 - 15	Alto

Número de respuestas afirmativas:	
Probabilidad inicial estimada:	

Riesgo inicial

Una vez estimado el impacto y la probabilidad inicial, aplique la matriz de riesgos vista anteriormente para calcular el riesgo inicial (sin los controles de seguridad).

Impacto en la confidencialidad Impacto en la integridad Impacto en la disponibilidad	
Impactos máximos Probabilidad	
Riesgo inicial	

Medidas de seguridad

Una vez calculado el riesgo inicial, es necesario determinar qué medidas para mejorar la seguridad deben aplicarse.

Hay muchas listas de medidas. Aquí hacemos uso de las medidas de seguridad que el ENS (Esquema Nacional de Seguridad) incluye en el anexo II de su guía[45] . Aplicaremos las medidas según nos indique la tabla para el valor del riesgo (bajo, medio, Alto o Muy Alto). Los riesgos altos o muy altos deben intentar reducirse siempre, por eso los hemos agrupado en la misma columna.

Bajo	Medio	Alto o Muy alto	Control	Aplicado
Marco organizativo				
Sí	Sí	Sí	Política de seguridad [org.1] (Sistema)	
Sí	Sí	Sí	Normativa de seguridad [org.2] (Sistema)	
Sí	Sí	Sí	Procedimientos de seguridad [org.3] (Sistema)	
Sí	Sí	Sí	Proceso de autorización [org.4] (Sistema)	
Marco operacional				
				Planificación
Sí	Sí	Sí	Arquitectura de seguridad [op.pl.2] (Sistema)	
Sí	Sí	Sí	Adquisición de nuevos componentes [op.pl.3] (Sistema)	
No	Sí	Sí	Dimensionamiento [op.pl.4] (D)	
No	No	Sí	Componentes certificados [op.pl.5] (Sistema)	
				Control de acceso
Sí	Sí	Sí	Identificación [op.acc.1] (Sistema)	
Sí	Sí	Sí	Requisitos de acceso [op.acc.2] (ICAT)	
No	Sí	Sí	Segregación de funciones y tareas [op.acc.3] (ICAT)	
Sí	Sí	Sí	Proceso de gestión de derechos de acceso [op.acc.4] (ICAT)	
Sí	Sí	Sí	Mecanismo de autenticación [op.acc.5] (ICAT)	
Sí	Sí	Sí	Acceso local [op.acc.6] (ICAT)	
Sí	Sí	Sí	Acceso remoto [op.acc.7] (ICAT)	
				Explotación
Sí	Sí	Sí	Inventario de activos [op.exp.1] (Sistema)	
Sí	Sí	Sí	Configuración de seguridad [op.exp.2] (Sistema)	

[45] Verificación del cumplimiento del ENS: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

No	Sí	Sí	Gestión de la configuración [op.exp.3] (Sistema)	
Sí	Sí	Sí	Mantenimiento [op.exp.4] (Sistema)	
No	Sí	Sí	Gestión de cambios [op.exp.5] (Sistema)	
Sí	Sí	Sí	Protección frente a código dañino [op.exp.6] (Sistema)	
No	Sí	Sí	Gestión de incidentes [op.exp.7] (Sistema)	
No	No	Sí	Registro de la actividad de los usuarios [op.exp.8] (Sistema)	
No	Sí	Sí	Registro de la gestión de incidentes [op.exp.9] (Sistema)	
No	No	Sí	Protección de los registros de actividad [op.exp.10] (Sistema)	
No	No	Sí	Protección de claves criptográficas [op.exp.11] (Sistema)	
			Servicios externos	
No	Sí	Sí	Contratación y acuerdos de nivel de servicio [op.ext.1] (Sistema)	
No	Sí	Sí	Gestión diaria [op.ext.2] (Sistema)	
No	Sí	Sí	Medios alternativos [op.ext.3] (D)	
			Continuidad del servicio	
No	Sí	Sí	Análisis del impacto [op.cont.1] (D)	
No	No	Sí	Plan de Continuidad [op.cont.2] (D)	
No	No	Sí	Pruebas periódicas [op.cont.3] (D)	
			Supervisión del sistema	
No	No	Sí	Detección de intrusión [op.mon.1] (Sistema)	
No	No	Sí	Sistema de métricas [op.mon.2] (Sistema)	
Medidas de protección				
			Protección de instalaciones e infraestructuras	
Sí	Sí	Sí	Áreas separadas y con control de acceso [mp.if.1] (Sistema)	
Sí	Sí	Sí	Identificación de las personas [mp.if.2] (Sistema)	
Sí	Sí	Sí	Acondicionamiento de los locales [mp.if.3] (Sistema)	
No	Sí	Sí	Energía eléctrica [mp.if.4] (D)	
Sí	Sí	Sí	Protección frente a incendios [mp.if.5] (D)	
No	Sí	Sí	Protección frente a inundaciones [mp.if.6] (D)	
Sí	Sí	Sí	Registro de entrada y salida de equipamiento [mp.if.7] (Sistema)	
No	No	Sí	Instalaciones alternativas [mp.if.8] (D)	
			Gestión del personal	
No	No	Sí	Caracterización del puesto de trabajo [mp.per.1] (Sistema)	
Sí	Sí	Sí	Deberes y obligaciones [mp.per.2] (Sistema)	
Sí	Sí	Sí	Concienciación [mp.per.3] (Sistema)	
Sí	Sí	Sí	Formación [mp.per.4] (Sistema)	
No	No	Sí	Personal alternativo [mp.per.5] (D)	
Protección del equipo				
No	Sí	Sí	Puesto de trabajo despejado [mp.eq.1] (Sistema)	
No	Sí	Sí	Bloqueo de puesto de trabajo [mp.eq.2] (Sistema)	
No	Sí	Sí	Protección de equipos portátiles [mp.eq.3] (Sistema)	
No	Sí	Sí	Medios alternativos [mp.eq.4] (D)	
			Protección de las comunicaciones	
Sí	Sí	Sí	Perímetro seguro [mp.com.1] (Sistema)	
No	Sí	Sí	Protección de la confidencialidad [mp.com.2] (C)	
Sí	Sí	Sí	Protección de la autenticidad y de la integridad [mp.com.3] (IA)	
No	No	Sí	Segregación de redes [mp.com.4] (Sistema)	
No	No	Sí	Medios alternativos [mp.com.5] (D)	
			Protección de los medios de información	
Sí	Sí	Sí	Etiquetado [mp.si.1] (C)	
No	Sí	Sí	Criptografía [mp.si.2] (IC)	
Sí	Sí	Sí	Custodia [mp.si.3] (Sistema)	
Sí	Sí	Sí	Transporte [mp.si.4] (Sistema)	
No	Sí	Sí	Borrado y destrucción [mp.si.5] (C)	
			Protección de aplicaciones informáticas	
No	Sí	Sí	Desarrollo de aplicaciones [mp.sw.1] (Sistema)	
Sí	Sí	Sí	Aceptación y puesta en servicio [mp.sw.1] (Sistema)	

				Protección de la información
Sí	Sí	Sí	Calificación de la información [mp.info.2] (C)	
No	No	Sí	Cifrado [mp.info.3] (C)	
Sí	Sí	Sí	Firma electrónica [mp.info.4] (IA)	
No	No	Sí	Sellos de tiempo [mp.info.5] (T)	
Sí	Sí	Sí	Limpieza de documentos [mp.info.6] (C)	
No	Sí	Sí	Copias de seguridad [mp.info.7] (D)	
				Protección de los servicios
Sí	Sí	Sí	Protección de correo electrónico [mp.s.1] (Sistema)	
Sí	Sí	Sí	Protección de servicios y aplicaciones web [mp.s.2] (Sistema)	
No	Sí	Sí	Protección frente a la denegación de servicio [mp.s.3] (D)	
No	No	Sí	Medios alternativos [mp.s.9] (D)	

Impacto residual

Las comprobaciones de seguridad pueden reducir el impacto de un incidente de seguridad. Por ejemplo, el cifrado de cierta información puede limitar el alcance de una pérdida de confidencialidad, una copia de seguridad puede limitar el impacto de una pérdida de disponibilidad de información y el uso de firma electrónica puede permitir la detección y, por lo tanto, la reducción del impacto, de una pérdida de integridad.

Impacto que la pérdida de confidencialidad de los datos (es decir, del acceso no autorizado a los datos) tiene sobre las personas.
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Impacto residual ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

Impacto que la pérdida de la integridad de los datos (es decir, de la modificación no autorizada de los datos) tiene sobre las personas.
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Impacto residual ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

Impacto que la pérdida de disponibilidad de datos tiene en las personas.
Impacto ☐Bajo ☐Medio ☐Alto ☐Muy alto
Impacto residual ☐Bajo ☐Medio ☐Alto ☐Muy alto
Justificación

El impacto residual del sistema será el máximo de los tres anteriores.

Impacto residual del sistema
☐Bajo ☐Medio ☐Alto ☐Muy alto

Probabilidad residual

Para reducir la probabilidad, es necesario eliminar los casos que hacen que las preguntas en el apartado anterior de la "probabilidad inicial" tengan respuestas afirmativas. Por ejemplo, si permitir el tratamiento a través de internet no es esencial, podemos desactivarlo para hacer que la respuesta a la pregunta P2 sea negativa.

Muchas veces no es factible eliminar los casos asociados a todas las preguntas de ese apartado. En ese caso, para cambiar de una respuesta afirmativa a negativa, hay que justificar que, en el contexto del sistema de tratamiento, los controles implementados hacen que el objeto de la pregunta tenga un peso despreciable en la aparición de incidentes de seguridad.

Es necesario revisar las respuestas dadas en el cálculo de la probabilidad inicial teniendo en cuenta las medidas de seguridad implementadas.

Hardware y software		
P1	**¿El sistema de tratamiento está conectado a sistemas externos a la organización?** Controles y justificación implementados	☐Sí ☐No
P2	**¿Alguna parte del tratamiento se realiza a través de Internet?** Controles y justificación implementados	☐Sí ☐No
P3	**¿Falta de seguimiento de un documento de buenas prácticas relevante en el diseño o configuración del sistema de tratamiento?** Controles y justificación implementados	☐Sí ☐No
P4	**¿Falta de seguimiento de un documento de buenas prácticas relevante en el mantenimiento, la monitorización y la respuesta a incidentes del sistema de tratamiento?** Controles y justificación implementados	☐Sí ☐No
P5	**¿Hay falta de seguridad física en las instalaciones donde se lleva a cabo el tratamiento?** Controles y justificación implementados	☐Sí ☐No

Procedimientos relacionados con el tratamiento		
P6	**¿Hay falta de claridad en la definición de las funciones y responsabilidades de los trabajadores?** Controles y justificación implementados	☐Sí ☐No
P7	**¿Hay falta de claridad a la hora de definir los usos aceptables de los sistemas de tratamiento?** Controles y justificación implementados	☐Sí ☐No
P8	**¿Puede el personal conectar dispositivos externos al sistema?** Controles y justificación implementados	☐Sí ☐No
P9	**¿Existe un procedimiento adecuado de registro y supervisión de las actividades relacionadas con el tratamiento?** Controles y justificación implementados	☐Sí ☐No

Personas involucradas en el tratamiento		
P10	**¿El personal recibe permisos que no son necesarios para cumplir con las tareas encomendadas?** Controles y justificación implementados	☐Sí ☐No
P11	**¿Alguna parte del tratamiento ha sido subcontratada a un encargado?** Controles y justificación implementados	☐Sí ☐No
P12	**¿Existe un desconocimiento del personal sobre el uso adecuado del sistema, de los aspectos de la seguridad de los datos o de las limitaciones de uso impuestas por el RGPD?** Controles y justificación implementados	☐Sí ☐No

Otras características		
P13	**¿Ha sufrido la empresa u otras empresas del sector ataques últimamente?**	☐Sí ☐No
P14	**¿Se han recibido quejas de alguien sobre la estabilidad o seguridad del sistema de tratamiento últimamente?**	☐Sí ☐No
P15	**¿Se tratan datos de especial interés o datos de un gran número de usuarios?**	☐Sí ☐No

La probabilidad residual se calcula contando el número de respuestas afirmativas.

Respuestas afirmativas	Probabilidad inicial
0 - 4	Bajo
5 – 9	Promedio
10 - 14	Alto

Estimación del riesgo residual

Una vez estimado el impacto y la probabilidad residuales, calculamos el riesgo residual de acuerdo con la matriz de riesgos que hemos visto antes.

Probabilidad					
	Máxima	Riesgo medio	Riesgo alto	Riesgo muy alto	Riesgo muy alto
	Significativa	Riesgo medio	Riesgo medio	Riesgo alto	Riesgo muy alto
	Limitada	Riesgo bajo	Riesgo medio	Riesgo medio	Riesgo alto
	Despreciable	Riesgo bajo	Riesgo bajo	Riesgo medio	Riesgo medio
		Despreciable	Limitado	Significativo	Máximo
		Impacto			

Impacto residual en la confidencialidad Impacto residual en la integridad Impacto residual en la disponibilidad	
Impactos residuales máximos Probabilidad residual	
Riesgo residual	

Si el riesgo residual es alto, es necesario proponer nuevos controles para reducirlo. Si no es posible reducirlo, antes de iniciar el tratamiento es necesario consultar a la autoridad competente de protección de datos sobre su idoneidad.

PLAN DE ACCIÓN Y CONCLUSIONES

Para tener disponibles a simple vista las medidas tomadas a lo largo de la EIPD para conseguir reducir los riesgos hasta un nivel aceptable, podemos incluirlas en esta sección

Resumen medidas implementadas:

Responsable que ha implantado las medidas:

Conclusiones:

SUPERVISAR Y REVISAR LA IMPLANTACIÓN

Programar revisiones periódicas para revisar que la implantación de la actividad de tratamiento siga teniendo unos niveles de riesgos aceptables.