UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía para la realización del Privacy Impact Assessment (PIA, Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Montesinos Rodrigo, Laura

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2021/2022

Resumen

Hace ya muchos años que se le da gran importancia a proteger los datos fundamentales de los ciudadanos en relación con la informática. Se considera un derecho fundamental desde la Constitución Española de 1978, y desde 1994 funciona la Agencia Española de Protección de Datos.

Más tarde, en 2018, entra en funcionamiento el Reglamento General de Protección de Datos, haciendo que toda Europa se rija por el mismo marco normativo.

En el presente trabajo se habla, desde la historia de la protección de datos, hasta las novedades más recientes de los nuevos reglamentos y los cambios que estos conllevan. Además, se hace especial hincapié en tratar de diseñar una hoja de ruta a utilizar en las Evaluaciones de Impacto referentes a la Protección de Datos y su correspondiente gestión de riesgos, incluyendo formas de reducirlos y mitigarlos.

Con este trabajo, se pretende ayudar y orientar a todo responsable y encargado de los tratamientos de datos, para que, con él, puedan apoyar su trabajo o saber qué herramientas son las más recomendadas para realizarlo.

Se concluye el trabajo con un ejemplo de Evaluación de Impacto referente a la Protección de Datos muy reciente. Se estudia la creada para la aplicación Radar COVID-19.

Palabras clave: protección, datos, RGPD, riesgo, impacto, AEPD, evaluación, COVID, EIPD

Abstract

For many years now, great importance has been attached to protecting the fundamental data of citizens in relation to computing. It is considered a fundamental right since the Spanish Constitution of 1978, and since 1994 the Spanish Data Protection Agency, AEPD, has been operating.

Later, in 2018, the General Data Protection Regulation, RGPD, came into operation, making all of Europe governed by the same regulatory framework.

The present work, we talk about, from history of data protection, to the most recent developments of the new regulations and the changes that these entail. In addition, special emphasis is placed on trying to design a roadmap to be used in Impact Assessments regarding Data Protection and its corresponding risk management, including ways to reduce and mitigate them.

With this work, it is intended to help and guide all those responsible and in charge of data processing, so that, with it, they can support their work or know which tools are the most recommended to carry it out.

The work is concluded with an example of an Impact Assessment referring to very recent Data Protection. The one created for the Radar COVID-19 application is studied.

Keywords : protection, data, RGPD, risk, impact, AEPD, evaluation, COVID, PIA

Resum

Fa ja molts anys que se li dóna gran importància a protegir les dades fonamentals dels ciutadans en relació amb la informàtica. Es considera un dret fonamental des de la Constitució Espanyola de 1978, i des de 1994 funciona l'Agència Espanyola de Protecció de Dades.

Més tard, en 2018, entra en funcionament el Reglament General de Protecció de Dades, fent que tota Europa es regisca pel mateix marc normatiu.

En el present treball es parla, des de la història de la protecció de dades, fins a les novetats més recents dels nous reglaments i els canvis que estos comporten. A més, es fa especial insistència a tractar de dissenyar un full de ruta a utilitzar en les Avaluacions d'Impacte referents a la Protecció de Dades i la seua corresponent gestió de riscos, incloent formes de reduir-los i mitigar-los.

Amb aquest treball, es pretén ajudar i orientar tot responsables i encarregats dels tractaments de dades, perquè, amb ell, puguen recolzar el seu treball o saber quines ferramentes són les més recomanades per a realitzar-ho.

Es conclou el treball amb un exemple d'una Avaluació d'Impacte relativa a la Protecció de Dades que ens toca de manera recent. S'estudia la creada per a l'aplicació Radar COVID-19.

Paraules clau: protecció, dades, RGPD, risc, impacte, AEPD, avaluació, COVID, AIPD

Índice de figuras

Lista de tablas

Tabla de contenidos

1. Introducción

Muy pocas veces se para a pensar detenidamente en la importancia que tienen los datos y qué se está haciendo con ellos. El mundo está rodeado de datos y de dispositivos a los que se les confían los datos sin pensarlo dos veces.

Además, la mayoría de los dispositivos que se utilizan diariamente, y cada vez en mayor medida, están conectados a Internet, incluso los electrodomésticos del hogar. Por tanto, todos los datos que se almacenan en estos dispositivos están también conectados a Internet.

Datareportal realiza anualmente un informe global digital en colaboración con We Are Social y Hootsuite. Se trata de un informe muy completo sobre redes sociales, el comercio electrónico, el contenido de transmisión y los videojuegos. Sirve para corroborar la información mencionada. En la figura 1, se muestra la información de enero de 2022, en la que se puede ver como el 62,5% de la población, casi 5 billones de personas, utilizan Internet, y por tanto, prácticamente todos ellos hacen uso de las redes sociales, concretamente el 58,4% de la población, según DataReportal. Todo esto supone un crecimiento mayor al 10% respecto al ejercicio anterior, 2021.

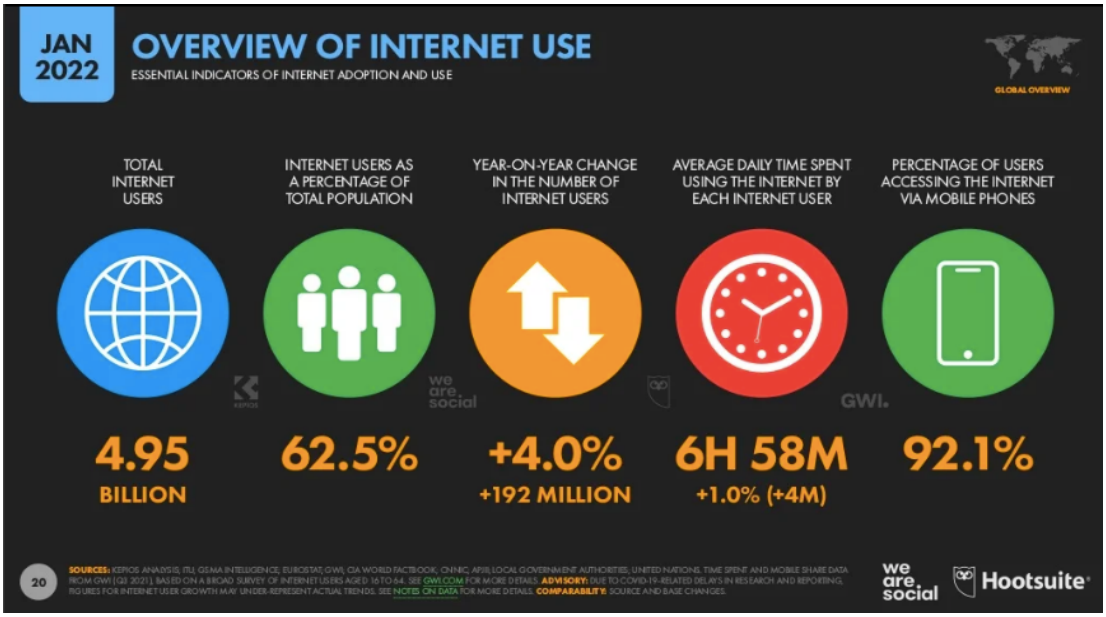

Figura 1. Overview of Internet Use

Fuente: Datareportal, 2022

Lo más importante que se debe saber a la hora de conectarse a la red, es que hay que proteger los datos personales, ya que todas las plataformas trabajan con los datos de sus usuarios e incluso llegan a ser su principal fuente de ingresos.

Como se ha visto, el 58,4% de la población participa activamente en redes sociales, generalmente, todas estas personas, ingresan todos los datos que se les pide sin tener en cuenta el riesgo que esto conlleva, y dónde pueden llegar a terminar todos esos datos.

Por todo ello, es muy importante conocer las leyes que protegen a las personas de estos riesgos y hacen conocer los derechos personales sobre el intercambio de los datos, una vez se han cedido.

En este trabajo se hablará sobre las leyes de protección y contención de datos de personales, sobre todo en España, donde desde mayo de 2018 está vigente el Reglamento General de Protección de Datos[1] (UE 2016/679), de ahora en adelante RGPD y del mismo año, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, a partir de ahora LOPDGDD.

El RGPD es obligatorio a nivel europeo y exige el cumplimiento de ciertos requerimientos novedosos para los responsables del tratamiento.

Entre estas obligaciones destaca la de evaluar el impacto relativo a proteger los datos, cuando el tratamiento de estos datos pueda ser un problema arriesgado para las libertades y derechos de las personas.

Por lo tanto, el presente trabajo de fin de grado plantea las circunstancias en las que es necesaria una guía para ayudar a la elaboración Evaluaciones de Impacto referentes a la Protección de Datos, a partir de ahora, PIA[2], por sus siglas en inglés o EIPD, para responsables y encargados del tratamiento de datos, así como la forma de realizarla.

[1] Reglamento General de Protección de Datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

[2] PIA: Privacy Impact Assessment

1.1. Motivación

La elección de este trabajo viene motivada por el interés personal por la importancia sobre la protección de datos personales.

Con solo fijarse un mínimo, cada día se puede ver que se está rodeado de datos personales, pero a la vez, de derechos que protegen a los ciudadanos cuando se ceden los mismos. Seguramente el lector haya aceptado un largo texto que habla sobre todo esto al iniciar cualquier aplicación, dispositivo, o incluso contrato. Y, además, habrá recibido numerosos correos recordándole la política de privacidad que ha aceptado en los lugares en los que ha depositado sus datos. Y posiblemente, se haya obviado todo esto, pensando que no era para nada importante, pero sí lo era.

Recientemente, se hizo viral la entrada en vigor de una nueva política de privacidad de WhatsApp. La aplicación dio como límite para aceptar dicha política hasta el 15 de mayo de 2021, en caso contrario, las cuentas no se borraban, pero tendrían una funcionalidad limitada.

Esta noticia causó mucho revuelo y dudas en los usuarios, debido a los cambios que ocasiona: nuevas opciones para chatear con empresas o realizar compras directamente desde Whatsapp, entre otros. Además, se remarcó que WhatsApp comparte información con otras empresas pertenecientes a Meta Platforms, y aunque esta información no sean los mensajes, llamadas o archivos que comparten entre sí los usuarios, si lo es tanto el número de teléfono como diversa información del dispositivo móvil y la dirección IP, entre otros datos.

Aun así, se ha demostrado que la nueva política cubre legalmente la nueva funcionalidad del contacto con empresas: “toda la información que WhatsApp comparta de este modo, no puede utilizarse para los fines propios de las empresas de Facebook”.

Además, en el caso de Europa, los cambios no afectan lo más mínimo, ya que, para la Unión Europea, WhatsApp tiene sede en Irlanda, y se rigen por el RGPD, que como relata la noticia, es “la legislación internacional más restrictiva en materia de privacidad” (RTVE, 2021).

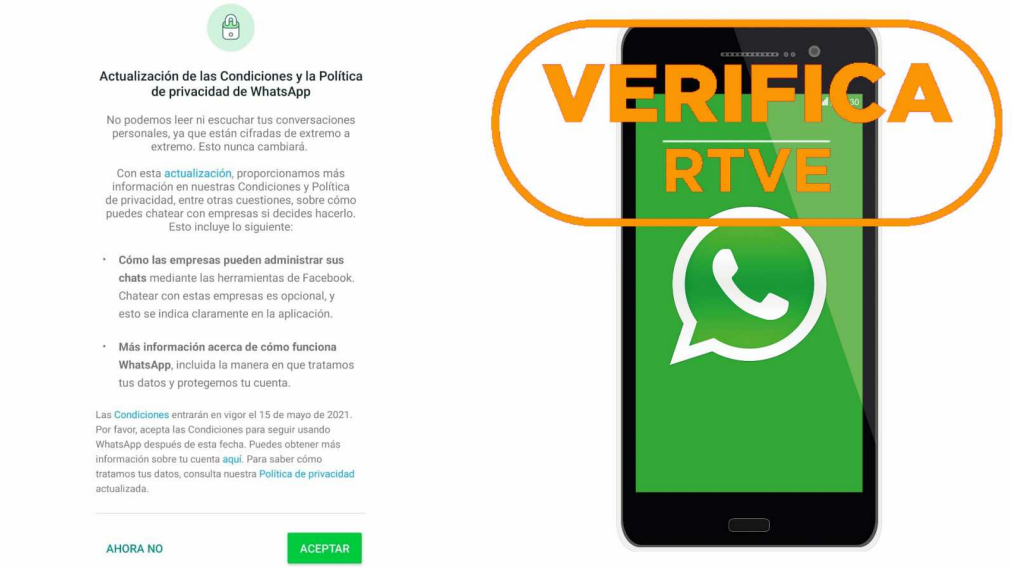

Figura 2. Novedades de WhatsApp desde el 15 de mayo

Fuente: VerificaRtve, 2021

A raíz de los cambios legislativos mencionados, y también del crecimiento que está teniendo el uso diario de las redes sociales, es importante saber, por una parte, los derechos que tienen los usuarios al ceder los datos personales y por otra, la forma y las obligaciones que conlleva este tratamiento de datos para los responsables del mismo, con sus novedades legales.

1.2. Objetivos

Como ya se ha mencionado, el **principal objetivo** del presente trabajo es crear una guía que ayude a los responsables de tratar los datos personales a elaborar la Evaluación de Impacto respetando el cumplimiento normativo, en el caso de que sea necesaria.

Por tanto, se informará en primer lugar de la historia que tiene la legislación sobre protección de datos para poner en contexto al lector. Con esto, se verán las novedades que se han incorporado y la actualidad de la mencionada legislación.

Entre dichas novedades, se encuentran dos de gran importancia, la **responsabilidad proactiva**, que se detalla más adelante, y la cual obliga a los responsables a un cumplimiento rígido de las medidas impuestas. Y, por otro lado, la necesidad para los mismos responsables de ampliar sus conocimientos sobre la EIPD. Se otorga gran importancia, incluso más que antes, a garantizar los derechos y libertades de las personas interesadas, y ahí es donde se hará más hincapié.

Por tanto, los **objetivos específicos** del trabajo serán:

-Analizar el contenido del nuevo reglamento

-Conocer guías y herramientas ofrecidas por las autoridades de control, la AEPD, entre otras, que serán instrumentos útiles para los responsables y encargados

-Aprender a realizar una correcta y completa gestión de los riesgos, proporcionando ayudas o apoyos que puedan servir a los responsables en todas las fases de esta gestión

-Proporcionar las pautas recomendadas por las instituciones para adaptarse al RGPD

-Ejemplificar la manera de realizar la EIPD

Y con todo esto, se pretende obtener un trabajo que ayude a los profesionales de la protección de datos en su labor.

1.3. Estructura

Una vez ya claros los objetivos que va a cumplir el presente trabajo y habiendo introducido el tema a tratar, se va a explicar brevemente qué se va a encontrar en los siguientes capítulos.

En el capítulo 2, se habla del estado del arte, que va a incluir todos los antecedentes de la protección de datos. Primero se explica la historia, incluyendo todas las leyes y citas que puedan ser de interés. Después, se habla de los últimos años, concretamente desde 2018, donde se encuentra el cambio significativo y que ha llevado a realizar este trabajo. Además de explicar la historia actual, se explican las novedades que trae la legislación y las libertades y derechos de los interesados. A la vez, se explica el término

responsabilidad proactiva y se dan diez pautas que se deben seguir para adaptarse a las novedades mencionadas anteriormente que trae el RGPD.

Después, se habla del análisis de riesgos en los tratamientos con el apoyo de la Agencia Española de Protección de Datos[3], la AEPD a partir de ahora, imprescindible en este tema, y de la forma de llevar el análisis a cabo.

Para terminar el capítulo, se introduce la Evaluación de Impacto en la Protección de Datos Personales, para saber en qué consiste, las etapas que tiene y quién serán los encargados de llevarla a cabo.

En el capítulo 3, se habla en profundidad de la propuesta del trabajo. Como ya se ha mencionado, la propuesta es crear una guía que apoye a los responsables y encargados de realizar la EIPD. Se detallan en profundidad todas las fases de ejecución de la misma, después se habla de las Autoridades de control que existen, y que proporcionan diversas herramientas y guías para ayudar al responsable del tratamiento. Y para terminar el capítulo, se habla de un ejemplo sobre la realización de una EIPD. En este caso, se ha considerado interesante, dados los últimos acontecimientos, hablar sobre la aplicación Radar COVID-19, creada a mediados de 2020 y de la cual se realizó una EIPD a finales de ese mismo año.

En el capítulo 4, se sacan las conclusiones finales del trabajo y se revisa si se han cumplido los objetivos propuestos.

Para acabar, en el capítulo 5 se pueden encontrar todas las referencias bibliográficas consultadas y en el capítulo 6, los anexos que se irán mencionando a lo largo del trabajo y que sirven de apoyo para realizar la tarea de los responsables.

1.4. Limitaciones

Dado que se trata de un trabajo relacionado con protección de datos, se incluyen numerosas leyes, normas, definiciones y temas, comunes a trabajos presentados sobre

[3]Agencia Española de Protección de Datos https://www.aepd.es/es

este mismo tema, la protección de datos, concretamente la evaluación de impacto de esta.

Se pueden encontrar por tanto, numerosas coincidencias con páginas y artículos que hablan sobre el mismo tema, la Evaluación, y que también han obtenido información de las completas guías que ofrece la AEPD. En nuestro caso se han incluido todas las referencias bibliográficas de las que se ha utilizado información diversa como definiciones o leyes.

NOTA IMPORTANTE: además de lo que se acaba de mencionar, tras subir el documento sin finalizar a una tarea de turnitin que no estaba preparada para no guardar el registro en la base de datos y perteneciente a otra cuenta, se detecta el mismo trabajo como plagio. Se puede observar el primer registro del informe, así como los cambios realizados sobre ese primer documento. Y se mostrarán ejemplos de lo mismo al inicio de la defensa.

Si se revisa el informe ofrecido por Turnitin se podrá comprobar lo mencionado anteriormente.

2. Estado del arte

Aunque desde mayo de 2018 está en vigor el RGPD, la situación anterior en cuanto a leyes y regulaciones ha sido muy variada y es interesante conocerla antes de estudiar la situación actual.

Las leyes se han ido adaptando a la evolución de las tecnologías y al aumento en el uso de los datos personales, como se ha comentado en la introducción.

2.1. Historia de la legislación

La historia de la legislación en materia de protección de los datos personales hasta que llega el RGPD, comienza en una Asamblea General de las Naciones Unidas en París el

10 de diciembre de 1948, con el artículo 12 de la Declaración Universal de Derechos Humanos:

«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. Todas las personas tienen derecho a la protección de la ley contra tales injerencias o ataques.» (art. 12 DUDH).

Más tarde, el Convenio Europeo de Protección de los Derechos Humanos y Libertades Fundamentales, el 4 de noviembre de 1950, enunciaba en su 8º artículo:

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

Y unos años más tarde entra en vigor en España la Constitución Española de 1978, una norma suprema de ordenamiento jurídico que hacía mención de la privacidad en los artículos 18.1 y 18.4:

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

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

El Convenio 108 del Consejo de Europa del 28 de enero de 1981, "*para proteger de toda persona con respecto al tratamiento automático de los datos personales",* establece en su artículo 1:

«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, en referencia al tratamiento automático de los datos de carácter personal correspondientes a dicha persona ("protección de datos")» (art. 1 C108).

El 29 de octubre de 1992 se aprueba en España la Ley Orgánica 5/1992, de *Regulación del Tratamiento Automatizado de los Datos de carácter personal*, la LORTAD, a partir de ahora en el resto del documento. Desde entonces, quedan amparados por la ley, los derechos de privacidad, protección e intimidad de los datos. Además, surge la "Agencia Española de Protección de Datos" como autoridad independiente de control.

En la Unión Europea, se aprueba el 24 de octubre de 1995 la Directiva 95/46/CE sobre "*proteger a personas físicas respecto a la trata de datos personales y su libre circulación"*, y es la primera ley inclusiva que permite intercambiar datos entre los países que pertenecen a la Unión Europea. Esta ley establece un plazo de tres años para ser traspuesta al ordenamiento interno de cada Estado miembro. En 1999, España traspuso esta ley. Se aprobó la Ley Orgánica 15/1999, del 13 de diciembre, de *Protección de Datos de Carácter Personal*, a partir de ahora, la LOPD. A raíz de este hecho, se deroga la LORTAD, gracias a la regulación del tratamiento de datos en soporte físico.

La LOPD es una ley que se crea con prisas, ya que contaba con el plazo establecido por la Unión Europea que terminaba en octubre de 1998. La ley entra en vigor fuera de plazo y está incompleta.

Por ello, hasta abril de 2008, la LOPD convive con numerosas disposiciones reglamentarias: el Real Decreto 1720/2007, de 21 de diciembre, y el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, "*referente a proteger de personas físicas en lo que refiere a la libre circulación y tratamiento de sus datos personales"*, a partir de ahora, el RGPD. Comienza a ser obligatorio el 25 de mayo de 2018 y se anula entonces la Directiva 95/46/CE.

El Reglamento se completa con la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, "*referente a proteger de las personas físicas en lo que respecta a la trata de datos personales por parte de las autoridades competentes para conseguir prevenir, investigar, enjuiciar o ejecutar sanciones penales o detectar infracciones penales, y a la circulación libre de dichos datos"* y el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, "*referente a un marco para la libre circulación de datos no personales de la Unión Europea"*.

Con esto, la normativa de toda Europa es la misma y queda uniforme. En el caso de España, se encontraban en vigor en ese momento tanto la LOPD como el RGPD, ambas sobre la protección de datos. El RGPD era mucho menos flexible.

Además, en ese momento había que adaptar el ordenamiento jurídico español, en este caso la LOPD, debía adaptarse al RGPD. Se aprueba entonces la elaboración de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, la LOPDGDD.

La LOPDGDD se compone de 97 artículos, divididos en 10 títulos, 22 disposiciones adicionales, 6 transitorias, 16 finales y 1 derogatoria. Incluye las medidas que impone el RGPD y algunas complementarias que mejoran aspectos de la LOPD, adaptándose a los tiempos.

La actualidad pues en España es desde 2018, la LOPDGDD junto al RGPD, se puede observar un cuadro resumen de la legislación española a lo largo del tiempo, mencionada anteriormente, en la Figura 3.

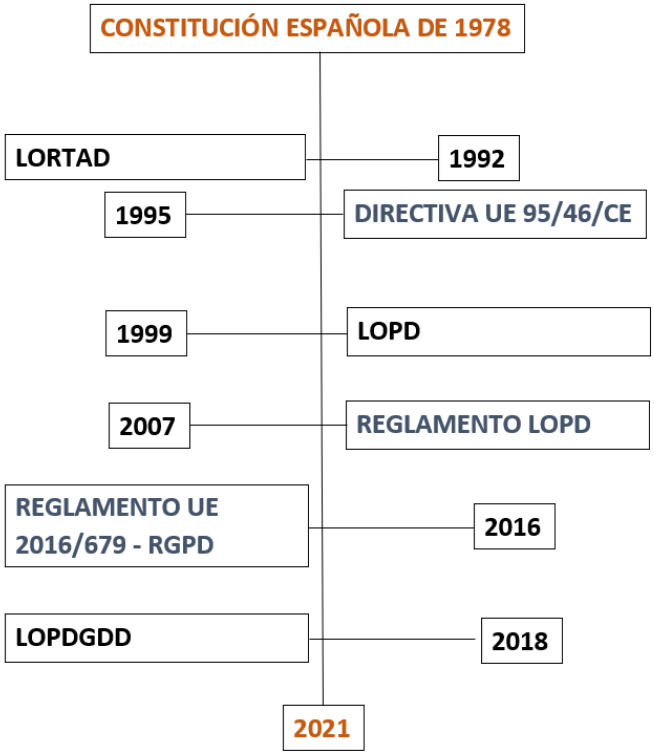

Figura 3. Leyes de Protección de datos españolas

Fuente: Elaboración propia

2.2. Datos de carácter personal

Antes de hablar sobre la ley actual, es momento de hablar sobre qué es un dato de carácter personal para la AEPD y para qué se utiliza, ya que es el término más importante del estudio que acompaña a lo largo de toda la memoria.

Tal como enuncia el RGPD, los **datos de carácter personal** son "*toda información sobre una persona física identificable o identificada. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo nombres, datos de localización, números de identificación, un identificador en línea o algún elemento propio de la identidad física, psíquica, genética, económica, fisiológica, cultural o social de dicha persona*".

Los datos se dividen en dos bloques, el primero, los datos especiales o sensibles y el segundo, los no sensibles. Entre los sensibles se encuentran, por ejemplo, los ideológicos, los relativos a la salud o los religiosos. Entre los no sensibles se encuentran principalmente los datos identificativos y, además, los financieros, profesionales, académicos, etc.

Algunos ejemplos de tipos de datos pueden ser los siguientes:

-Datos sensibles: características personales (estado civil, edad, sexo, nacionalidad…), circunstancias sociales (vivienda, propiedades, licencias…), opiniones políticas, vida sexual, orientación sexual, discapacidades, origen étnico, y muchos más.

-Datos no sensibles: identificativos (DNI, nombre, firma, dirección…), académicos o profesionales (formación, historial, experiencia…), de empleo (profesión, historial…), económicos o financieros (ingresos, renta, datos bancarios, seguros, beneficios…), de transacciones, de control de presencia, de personalidad u otros.

Como se puede intuir, los datos de carácter personal se usan a diario y en gran medida. Prácticamente se tienen que utilizar en todos los movimientos diarios: en los estudios, en el trabajo, en los centros médicos o en el ocio en general, tanto en suscripciones a servicios varios, como en reservas de vacaciones o en las redes sociales, utilizadas como se ha visto por la gran mayoría de la población.

Al ingresar estos datos de carácter personal, los responsables de su tratamiento, es decir, las empresas, Administraciones Públicas y otras entidades, deben cumplir con las obligaciones y principios que marca el RGPD.

Para comprender la importancia de los datos, es interesante el ejemplo de las nóminas de todos los trabajadores de las empresas, donde se incluye múltiple información. De estos documentos, se debe mantener la seguridad y garantizar su privacidad completa,

siguiendo así las implicaciones que establece el RGPD. Para ello, es común en multitud de empresas actualmente, cifrar mediante contraseña el documento que se envía al trabajador, como por ejemplo, su Documento de Identidad o incluso además, asignar un correo para que únicamente pueda abrirse el documento con esa dirección de correo.

2.3. Actualidad de la legislación

Aunque es importante conocer a grandes rasgos la historia de la legislación sobre protección de datos, lo más importante es saber en qué situación se encuentra actualmente. Para ello es necesario mencionar las novedades que incluyó la LOPDGDD en 2018 y las implicaciones que tiene el RGPD. Ambas se pueden consultar completas en la página oficial del ministerio.

Como ya se ha mencionado, la finalidad de la LOPDGDD es la protección de la intimidad, privacidad e integridad de los individuos, cumpliendo el artículo 18.4 de la Constitución Española. Además, regular toda obligación del individuo en la transferencia de datos para lograr la seguridad del intercambio.

2.3.1. Novedades legislativas

Se van entonces a comentar algunas de las novedades que incluye la LOPDGDD:

-**Tratamiento basado en el consentimiento del afectado (art.6 LOPDGDD)**: el consentimiento debe ser libre, informado, específico e inequívoco. Se debe considerar incuestionable y para ello debe existir una declaración de los interesados o una acción positiva que apunte al acuerdo, no se puede deducir la aceptación del silencio o la inacción del interesado. Y está relacionado también con el **Consentimiento de los menores de edad (art.7 LOPDGDD):** se establece la edad mínima a la que se permite dar consentimiento para tratar los datos personales es a los 14 años.

-Designar un delegado de protección de datos (art.34 LOPDGDD): en caso de que la responsabilidad del tratamiento de los datos corriese por parte de una autoridad pública, y si las principales operaciones del responsable fuesen el seguimiento regular

a gran escala y para estas operaciones, fuesen necesarios tratamientos a grandes escalas de datos personales que tienen que ver con delitos y condenas.

-Nuevos derechos digitales aprobados por el Congreso: Derecho a la neutralidad de Internet (art.80 LOPDGDD), acceso universal a Internet (art.81 LOPDGDD) o de seguridad digital (art.82 LOPDGDD), entre muchos otros.

-Derecho al olvido en servicios en redes sociales, búsquedas de Internet y servicios equivalentes (art.93 y 94 LOPDGDD): que permite al usuario reclamar aquellos datos presentes en Internet o en buscadores que tengan información obsoleta o desactualizada. Este derecho permite exigir su supresión.

-Medidas de responsabilidad activa. Obligaciones generales del encargado y responsable del tratamiento (art.28 LOPDGDD): se debe garantizar que los datos se tratan conforme al reglamento. Se debe valorar si procede, hacer la evaluación de impacto de la protección de datos, indagar en los riesgos que puede conllevar el sistema de información o el servicio respecto a la protección de datos, y este es el tema que interesa principalmente en este trabajo. Por tanto, se hará mayor hincapié en este punto más adelante.

Y tras comentar las novedades de la LOPDGDD, es importante mencionar brevemente también las nuevas normas del RGPD, que se corresponden siempre con un artículo de la LOPDGDD.

Las primeras novedades hablan sobre los derechos individuales de los interesados al ceder sus datos personales. Se detallan estos derechos en el “Capítulo III Derechos del interesado”, del artículo 12 al 23 del RGPD. Algunos de ellos son los siguientes:

-Derecho de acceso (art. 15 RGPD): cómo, hasta cuándo y con qué fin se tratan los datos.

-Derecho a la transparencia de la información (art. 12, 13 y 14 RGPD): identidad del responsable que va a tratar con los datos, qué tratamiento se va a realizar y la posible cesión de los mismos.

-Derecho a la portabilidad de los datos (art. 20 RGPD): para poder transferir la copia de los datos empleados por un primero a otro responsable.

-Derecho de supresión (Derecho al olvido) (art. 17 RGPD): para crear la posibilidad de que el interesado pueda hacer desaparecer sus datos de manera permanente, dando el derecho de revocar el consentimiento inicial.

-Derecho de rectificación (art. 16 RGPD): permite revisar los datos una vez cedidos.

-Derecho a limitar el tratamiento (art. 18 RGPD): suspender o limitar el uso de los datos, relacionado con el derecho al olvido.

-Derecho de oposición (art. 21 RGPD): oponerse al uso de los datos con un fin diferente al acordado.

Por otra parte, se encuentran las **novedades para los encargados y responsables** del tratamiento y procesamiento de estos datos. Esta parte es importante para el trabajo, ya que se centra en la realización de la EIPD según estos.

Esta información se encuentra en el "Capítulo IV encargado del tratamiento y responsable del tratamiento" del RGPD, del artículo 24 al 31. Los artículos 24 y 28 explican los roles:

-Encargado del tratamiento (art. 28): "*La persona física o jurídica, autoridad pública, servicio u otro organismo que haga el tratamiento de los datos personales por cuenta del responsable del tratamiento. Las obligaciones que tiene el encargado deberán quedar por escrito en un contrato formal, así como el registro de actividades que realice. Además, el responsable debe elegir un encargado que ofrezca plena garantía*".

-Responsable del tratamiento (art. 24): "*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 podrán establecerlos estos mismos*".

Se debe aclarar primero, qué es el tratamiento para el RGPD:

Se trata de "*cualquier operación u de operaciones sobre datos personales o conjuntos de datos personales, mediante procedimientos automatizados o no, como puede ser la recogida, el registro, la organización, estructuración, la conservación, cualquier forma de habilitación de acceso, cotejo o interconexión, adaptación o modificación, difusión,*

limitación, supresión o destrucción, extracción, utilización, comunicación por transmisión o consulta de los datos en cuestión".

Por otra parte, el artículo 5 habla sobre los "**principios referentes a la trata de los datos personales"** que corresponden a responsables y encargados.

Se expresa que los datos deben ser:

-Usados de manera lícita, leal y transparente

-Recogidos con fines legítimos y explícitos, y nunca con otros fines, excluyendo el de archivo interés público, de investigación científica o estadístico.

-Adecuados y limitados en referencia a la finalidad para la que se están tratando.

-Exactos y actualizados

-Mantenidos únicamente hasta que sea necesario, excluyendo también los fines mencionados en el primer punto de estos principios.

-Tratados de forma que se garantice su seguridad, asegurando su integridad y confidencialidad.

Además, el responsable del cumplimiento de estos principios será el que se encargue del tratamiento de los datos y debe ser capaz de demostrarlo, se trata de la **responsabilidad proactiva**.

La **responsabilidad proactiva** o **accountability** en inglés, es un término muy importante en este trabajo, ya que es la obligatoriedad de que los responsables apliquen las medidas apropiadas para garantizar que se cumple la normativa y, además, para demostrar el cumplimiento a los interesados y las autoridades. Esto implica que, a partir de este momento, con carácter previo al tratamiento, deben extremar la precaución de respetar los derechos e intereses de los ciudadanos con los que estén trabajando, en este caso los interesados.

Existen **diez pautas**, recomendadas por varias instituciones, como por ejemplo en la "Guía del Reglamento General de Protección de Datos para responsables de

tratamiento"[4] de la AEPD, que ayudan a adaptarse al RGPD más fácilmente a las organizaciones.

Pero antes de empezar cualquier actividad de tratamiento de datos, es necesario que exista una base jurídica que la certifique. Para que sea justo, se debe cumplir al menos una de las bases legales relatadas en el **artículo 6**: "*tener el consentimiento del interesado, ejecutar la relación contractual, que sea imprescindible para cumplir alguna obligación aplicable al responsable, ser necesario para proteger intereses vitales, para cumplir una misión realizada de interés público o para satisfacer los intereses legítimos del responsable o de terceros*".

Las pautas se pueden consultar detalladamente en los artículos que se irán mencionando, pero brevemente son las siguientes:

1 - Registrar las actividades del tratamiento (art. 30): como ya se ha mencionado antes, cada encargado y responsable debe tener un control de las actividades de tratamiento en las que sea responsable. Unos ejemplos de plantilla para registrar las actividades, tanto de encargado como de responsable, se pueden encontrar en la "Guía práctica sobre análisis de riesgos en los tratamientos de datos personales sujetos al RGPD"[5], y se adjuntan en esta memoria en los anexo 1 y 2 como ejemplos.

2 - Realizar un análisis de riesgos (art. 32): se debe corroborar que los tratamientos realizados no suponen riesgo para las libertades y derechos de los interesados. Y si es el caso, se deberán adoptar las medidas necesarias para minimizarlos. Este análisis deberá realizarse de manera periódica, y su tipo variará dependiendo del tipo de tratamiento, de la naturaleza de los datos, de la cantidad y variedad de tratamientos que la organización lleve a cabo y del número de interesados a los que afecta.

Para llevar a cabo esta tarea, el AEPD ofrece la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD". La guía detalla tres fases para realizar una gestión de los riesgos correcta.

---

[4] "Guía del Reglamento General de Protección de Datos para responsables de tratamiento" https://www.aepd.es/es/node/43452

[5] "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD"

https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

Las tres fases son: identificar las amenazas, evaluar los riesgos y tratarlos, para conseguir mitigarlos. Y como ya se ha mencionado, realizar esto de manera periódica.

3 - Proteger los datos desde el Diseño y por Defecto (Art. 25): antes de empezar el proceso de tratamiento y durante el desarrollo, el responsable debe darle importancia al principio de responsabilidad proactiva y a la importancia de las libertades y derechos de los interesados. Deben tomar medidas técnicas y organizativas que garanticen que sólo se usan los datos necesarios.

4 - Revisar las medidas de seguridad (Art. 32): desde la aplicación del RGPD, las medidas organizativas apropiadas deben ser establecidas por los responsables y encargados, y estas deben garantizar unos niveles de seguridad adecuados en función del nivel del riesgo detectado.

5 - Notificar cualquier "violación" de seguridad de los datos (Art 33 y 34): se trata de todo incidente que conlleve: perder, destruir o alterar los datos personales transmitidos o un acceso o comunicación a estos no autorizado. Se debe dar aviso a la autoridad que corresponde en un plazo máximo de 72 horas desde que el responsable sea consciente de ello. Para estos casos, el AEPD ofrece la "Guía para la gestión y notificación de brechas de seguridad"[6].

6 – Desarrollo de la Evaluación de Impacto sobre la Protección de Datos (Art. 35): los responsables del tratamiento están obligados a realizar la EIPD antes de realizar tratamientos que conlleven mucho riesgo para las libertades y los derechos de los interesados. En este trabajo, se va a profundizar en este tema y se va a realizar una guía para la realización del mismo. Por ello, se desarrollará en profundidad esta medida más adelante, pero aquí ya se puede ver la importancia que atañe al trabajo.

7 - Nombrar un Delegado de Protección de Datos (Art. 37-39): obligatorio en autoridades públicas, responsables de tratamiento con operaciones que supongan observar repetitiva y sistemáticamente a los interesados a grandes escalas y los que tengan entre sus actividades principales algunas con tratamiento a gran escala de datos

[6]"Guía para la gestión y notificación de brechas de seguridad" https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

sensibles. Pero, aunque no sea obligatorio, es aconsejable en todos los casos. Además la designación debe ser pública.

8 - Garantizar a los interesados el derecho a la transparencia de la información (Art. 12-14): informar de forma breve, clara, comprensible, con fácil acceso y con lenguaje sencillo. Además, debe ser por escrito. Toda la información se puede consultar en la "Guía sobre el derecho a la información"[7] de la AEPD.

9 - Atender a los interesados en ejercer sus derechos: es gratuito y los responsables lo deben facilitar a los interesados, con mecanismos sencillos.

10 - Realizar los contratos entre responsables y encargados del tratamiento: vincula al encargado respecto al responsable y tiene que contener, como mínimo: respectivo al tratamiento su objeto, duración y finalidad, el tipo de datos personales del interesado, la obligación de tratar los datos únicamente siguiendo instrucciones del responsable, las condiciones de subcontratación, etc... Además, la AEPD ofrece una plantilla para redactar dicho contrato, las "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"[8].

Antes de entrar en contexto de privacidad, y en relación a la actualidad legislativa, es interesante para este desarrollo introducir de manera general el Esquema Nacional de Seguridad y poder comprobar la relación que tiene el mismo con la AEPD y con la privacidad de los datos.

2.4. El Esquema Nacional de Seguridad y la Privacidad

Es muy importante tener en cuenta la seguridad en los sistemas de información. Esta práctica es el concepto de ciberseguridad, que se encarga de proteger los programas y

[7]"Guía sobre el derecho a la información"

https://www.aepd.es/es/node/43451

[8]"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"

https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

sistemas de ataques digitales. Los profesionales encargados de controlar y evitar estos ataques, deber tener muy en cuenta la importancia de la confidencialidad de los datos. Los ataques a dichos datos pueden llegar a ser desde el acceso a los mismos hasta su completa destrucción.

En este marco, el Esquema Nacional de Seguridad, a partir de ahora el ENS, se encarga de proporcionar la política de seguridad en cuanto a acceso, integridad y veracidad de los datos, necesaria para utilizar medios electrónicos, asegurando la protección necesaria para la información. El ENS es de cumplimiento obligatorio para todas las Administraciones Públicas, y para todas las entidades privadas que presten servicios a las primeras, desde 2017. Todo lo relativo a privacidad, lo descarga en la Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales, la LOPDGDD.

El ENS surge en el año 2017 a raíz del trabajo de los Ministerios de Presidencia y Política Territorial y Administración Pública, en colaboración con el CCN, el Centro Criptológico Nacional.

En este contexto, es muy importante hablar sobre la importancia de la privacidad y Protección de Datos relacionando este tema con el presente trabajo.

Como se veía al inicio, la actualidad legislativa es la LOPDGDD junto al RGPD. Y dado que toda actividad de tratamiento que hagan los responsables o encargados, debe tener en cuenta las obligaciones interpuestas que exigen ambas, todo cambio que surja entorno a la AEPD, y en concreto en estas leyes actuales, afecta totalmente a la privacidad del ENS y a estos profesionales de la ciberseguridad.

La LOPDGDD enumera las medidas de seguridad necesarias para el ámbito del sector público, en la que se incluyen puntos de gran importancia relacionados con el ENS. Relata que, el ENS debe incluir las medidas necesarias para ser implantadas en el caso de tratamiento de datos, para evitar la pérdida, alteración o acceso. Y además, que los responsables de estos tratamientos, quedan obligados a aplicar estas medidas de seguridad correspondientes a los tratamientos.

Es por esto que, como se ha dicho, todo cambio que se desarrolle entorno a la AEPD, y sus actuales leyes, la LOPDGDD y el RGPD, debe ser de especial atención para los responsables de tratamiento, para el Esquema Nacional de Seguridad y por tanto para el CCN.

2.5. Análisis de riesgos

En la pauta número 2, de las mencionadas anteriormente en la actualidad legislativa, se ha visto que es muy importante realizar un análisis de los riesgos, que es la forma en la que se conocerá si se debe realizar una EIPD en los datos que a priori son de bajo riesgo.

Se denomina análisis básico de riesgos en los tratamientos, al análisis de riesgos que a priori, son de bajo impacto para las libertades y derechos de los interesados. Si se tiene conocimiento de que los datos son de alto riesgo, directamente se realiza una EIPD.

Por tanto, para explicar el análisis de riesgos, hay que apoyarse en la hoja de ruta que ofrece la AEPD, la "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD"[9]. Aunque hay otras guías ofrecidas por otras autoridades de control.

Para empezar, el análisis de riesgos es una obligación para los encargados y responsables, para así interponer medidas de seguridad y controlar las libertades y derechos de los interesados.

Como se ha comentado en la pauta número 2, la gestión de riesgos tiene tres etapas que se irán repitiendo, como se puede observar en la figura 4.

[9]"Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD"

https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

Figura 4. Etapas de la gestión de riesgos

Fuente: AEPD, 2021

El primer punto es **identificar tanto las amenazas como los riesgos,** el riesgo viene derivado de exponerse a la amenaza, por tanto, hay que saber identificar las amenazas principalmente. Dichas amenazas son factores de riesgo que pueden provocar un perjuicio o daño a los interesados. Son de tres tipos: modificar de forma no autorizada los datos, acceso ilegítimo a los datos y eliminación de datos.

Por tanto, el riesgo se considera la combinación de que se materialice la amenaza y las consecuencias negativas que puedan derivarse. Y el nivel depende de la probabilidad de que se materialice y del impacto que tendría.

En segundo lugar, se deben **evaluar los riesgos identificados,** se trata de considerar las situaciones en las que el riesgo se puede hacer efectivo. Consiste en evaluar el impacto que supone exponerse a la amenaza y la probabilidad de que se materialice. Y para valorar el impacto, hay que tener en cuenta los posibles daños que produciría dicha amenaza. Y con todo esto, se determina el nivel de riesgo.

El último paso sería **tratar los riesgos,** para reducir el nivel de exposición mediante medidas de control, y reducir el impacto de que se materialicen. Se trata con la finalidad de reducirlo o incluso mitigarlo, para conseguir como mínimo, que sea aceptable.

Estas tres etapas en bucle son muy comunes en las compañías hoy en día. Y el RGPD aprovecha las ventajas que ofrece.

El encargado y responsable de tratar los datos deben de aplicar medidas tanto organizativas como técnicas que garanticen que se cumplen los principios desde el diseño y por defecto, como se mencionaba en la pauta 3. Esto se debe llevar a cabo con medidas de control y de seguridad, como se relata en el artículo 32 del RGPD. Además, también deben de cumplir con lo descrito en el artículo 5 sobre las nuevas obligaciones que impone el RGPD, los principios referentes al tratamiento de los datos al definirlo, como pueden ser: licitud, lealtad y transparencia, minimización o exactitud entre otros.

Se debe garantizar en todo momento la responsabilidad proactiva que se ha descrito con anterioridad, definir las actividades y documentar todos los análisis que se realicen.

Existen diferentes análisis para determinar el tipo de riesgo de los tratamientos, utilizado para saber si es necesario realizar la EIPD. Para ello, existen diferentes alternativas, como por ejemplo la herramienta Facilita[10], para tratamientos que a priori son de escaso riesgo, herramienta que pone a disposición de las personas y entidades la AEPD.

Pero la metodología para determinar si es imprescindible llevar a cabo la evaluación, tiene dos partes: primero, el **Análisis de las listas de tratamientos previstos en la regulación (Art. 35.3-35.5)** y después, el **Análisis de la naturaleza, alcance, contexto y fines del tratamiento (Art. 35.1).**

En la **fase 1** ya se descartan varios supuestos en los que la regulación dice que es obligatorio realizar una EIPD y otros en los que queda excluida esta necesidad. En caso contrario, se pasa a la **fase 2,** donde se evalúan las características de las actividades. Se debe valorar tanto el alcance como la naturaleza, contexto y finalidades del tratamiento. Y valorando todas estas características, se sabrán separar los tratamientos que conllevan un alto riesgo.

En el caso de que las actividades tengan un alto riesgo, se deberá analizar si realmente es correcto que lo tiene y si es así, será necesario realizar una EIPD.

[10]Facilita 2.0 AEPD
https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDM1NDc0MjExNjI5ODQwNTAwODAz?updated=true

Pero ese último tema, se tratará con profundidad en el apartado 3 del trabajo, ahora se va a centrar el interés en el caso en que las actividades de tratamiento no requieran una evaluación por tener un nivel de riesgo bajo. Para estas actividades, además de documentar los motivos por los que se llega a la conclusión de que tienen un riesgo bajo, se realiza un análisis de mínimos que simplifica el proceso de análisis de riesgos.

Para empezar, se necesitan describir de manera adecuada las actividades de tratamiento, como se detalla en la pauta 1. Además, con los registros se verán las semejanzas entre algunas actividades para poder agruparlas, y por tanto, tendrán algunos riesgos comunes. Con esto se simplifica el trabajo de análisis y se establecen medidas de seguridad por defecto.

El responsable entonces, debe asegurar que se cumplen todas las normas desde que se recogen los datos hasta que se destruyen, con las fases que se detallan en la figura 5:

Figura 5. Ciclo de vida de los datos

Fuente: AEPD, 2021

-Captura de datos: obtener los datos para almacenarlos y después procesarlos. Puede ser mediante formulario en papel, web o encuestas, entre otros.

-Clasificación/Almacenamiento: clasificar y almacenar en los sistemas o archivos según las categorías establecidas. Ya sea en un formato físico o un sistema informático.

-Uso/Tratamiento: operaciones sobre los datos por procesamientos automáticos o manuales.

-Cesión/Transferencia a un tercero de datos para su tratamiento: se trata de transferencia, consulta, entrega, interconexión, comunicación, difusión o cualquier manera de acceder a los datos.

-Destrucción: eliminar los datos de los sistemas o archivos para que ya no se puedan recuperar.

En cada fase intervienen los mismos elementos, que son los siguientes:

-Actividades u operaciones: la materialización de una finalidad sobre los datos. Son los procedimientos que se hacen en cada una de las fases con los datos para llegar a una finalidad.

-Datos: es de gran importancia identificar en cada fase los datos tratados para establecer interrelaciones y dependencias entre operaciones de tratamiento. Además, asegurar el **principio de minimización de datos**.

-Intervinientes: personas físicas o jurídicas, implicadas en las actividades del tratamiento y cuyas funciones están definidas previamente. Y su participación puede suponer una amenaza.

-Tecnología: elementos tecnológicos implicados en el tratamiento a un alto nivel. Todas las distintas tecnologías, aplicaciones, dispositivos, etc...

Con toda la información se deben poder identificar las amenazas y valorar los riesgos a los que se exponen los datos personales.

Además, es recomendable realizar una tabla que cruce los cuatro elementos mencionados con cada una de las cinco fases de la figura 5. Con esa tabla se describen las actividades, un ejemplo de ella es la que se puede ver en la figura 6, que proporciona la AEPD, pero se trata de una tabla sencilla con lo que se ha comentado hasta ahora, fases y elementos intervinientes.

		CICLO DE VIDA DE LOS DATOS EN LAS OPERACIONES DEL TRATAMIENTO				
		Captura de datos	*Clasificación / Almacenamiento*	*Uso / Tratamiento*	*Cesión o transferencia de los datos a un tercero para su tratamiento*	*Destrucción*
ELEMENTOS QUE INTERVIENEN EN LAS OPERACIONES DE TRATAMIENTO	*Actividades del proceso*					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					

Figura 6. Plantilla del ciclo de vida de los datos

Fuente: AEPD, 2021

Es importante presentar material gráfico que ayude a identificar los elementos principales de manera visual y resumida. Una manera de hacerlo en este caso, podría ser mediante diagramas, si van a ayudar realmente a aportar claridad. Un ejemplo de diagrama se puede observar en la figura 7.

En el diagrama se puede ver claramente diferenciada la tarea de cada uno: interesado, responsable y encargado del tratamiento, así como el posible flujo a seguir, desde el registro por parte del usuario interesado, hasta llegar al probable borrado de datos, pasando por almacenaje, utilización y transferencia de esos datos, que puede ser realizado tanto por el responsable como por el encargado.

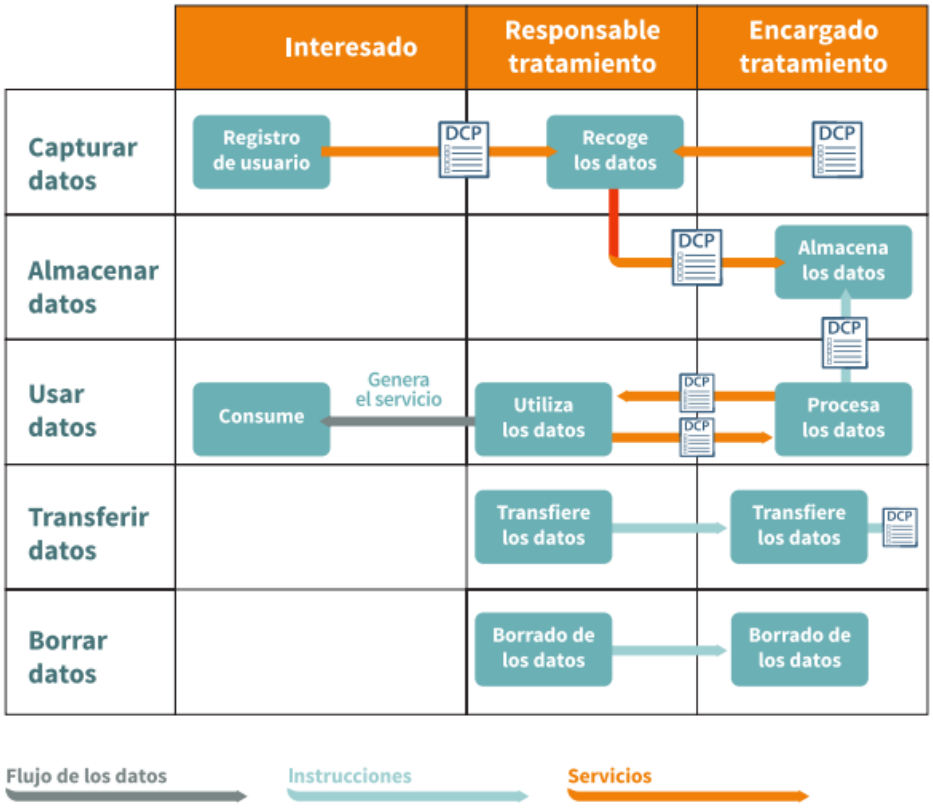

Figura 7. Diagrama de flujo como herramienta de apoyo

Fuente: AEPD, 2021

Una vez identificadas las amenazas, habría que evaluar los riesgos, pero en este caso no corresponde evaluarlos, ya que inicialmente los riesgos se han quedado en un nivel medio o bajo. Pero siempre hay que identificarlos y tratarlos.

Antes de analizarlos, hay que separar los tipos en dos dimensiones:

-Los referentes a la protección de la información de los datos: que afectan a su confidencialidad, lealtad y disposición.

-Relacionados con el cumplimiento de los requisitos regulatorios de las libertades y derechos de los interesados: cuando el interesado no puede hacer uso de sus derechos porque la organización que trabaja con sus datos no cuenta con los procedimientos correspondientes.

Cuando se identifica un riesgo bajo o medio con una actividad de tratamiento, hay que aplicar medidas de seguridad y control para reducir la exposición.

Los riesgos están relacionados con las amenazas a las que se expone la actividad, por tanto, hay que dar importancia a la descripción del tratamiento, de los elementos relevantes y de su contexto.

Por tanto, la forma de proceder en las actividades con riesgo bajo o medio para gestionarlos es: determinar cuáles son los riesgos, que dentro de las dimensiones, son de aplicación. Entonces, para esos riesgos se deben proponer medidas de seguridad que aseguren un control adecuado.

Los principales riesgos potenciales que se suelen identificar se pueden clasificar según lo siguiente:

-En los asociados a proteger de la información: **integridad, disponibilidad y confidencialidad de los datos personales.**

-En los asociados al cumplimiento: **garantizar los principios relativos al tratamiento y que los interesados ejerzan sus derechos.**

Algunos ejemplos de las medidas de control utilizadas para los riesgos expuestos se resumen en la tabla 1.

Tipo de riesgo	**Medidas de control**
Integridad	Control de monitorización de amenazas en red
Confidencialidad	Segmentación de la red y controles de acceso

Garantizar que los interesados ejercen de sus derechos	Procesos y canales para el ejercer de sus derechos
Disponibilidad	Realizar copia de seguridad y almacenar en un par de ubicaciones
Garantizar los principios referentes al tratamiento	Monitorizar el uso de datos personales o usar cláusulas informativas

Tabla 1. Medidas de control para rebajar la exposición al riesgo

Fuente: Elaboración propia a partir de AEPD, 2022

Tanto los riesgos identificados como las medidas de seguridad adoptadas, se deben de documentar, así se dará evidencia del análisis de riesgos que se ha realizado y se tendrá documentación ante futuras amenazas o revisiones que puedan ser similares.

Además, como ya se mencionó en la Figura 4 al hablar de las etapas, es muy importante la monitorización continua. Se requiere evaluación periódica de las medidas de control adoptadas, para detectar posibles variaciones en la actividad del tratamiento.

Para terminar esta parte, se adjunta en el anexo 3 una plantilla ejemplo para redactar el análisis de riesgos básico.

Tras esto, se llega a la casuística en la que sí sería necesario realizar una EIPD, para tratar bien esta parte, sirve de gran apoyo la "Guía de Evaluación de Impacto en la Protección de Datos"[11] ofrecida por la AEPD.

Como ya se ha mencionado antes, en el caso en que la actividad de tratamiento suponga un muy alto riesgo de cara a los interesados, es obligatorio realizarla.

[11]"Guía de Evaluación de Impacto en la Protección de Datos"
https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

2.6. Evaluación de Impacto en la Protección de Datos Personales

Para empezar, la EIPD se trata de una herramienta que debe crear el responsable y que evalúa anticipadamente los riesgos a los que se exponen o pueden exponer los datos según las actividades de tratamiento que vayan a tener (Art. 35 del RGPD). Además, la EIPD determina el nivel de riesgo de un tratamiento para saber qué medidas de control son las necesarias para reducir ese riesgo.

El resultado alcanzado con la EIPD es importante a la hora de tomar decisiones, sobre todo de la viabilidad de llevar a cabo el tratamiento. Es un informe con las características de las actividades, identificar los riesgos de las mismas y las decisiones que se han tomado para mitigarlos.

Los requerimientos que exige el RGPD para una EIPD como mínimo, según el artículo 35.7 del RGPD son:

-**Descripción sistemática** de la actividad

-**Evaluar la necesidad** del tratamiento en relación a la finalidad

-**Evaluar los riesgos**

-Medidas para conllevar los riesgos que garanticen la protección de datos personales.

2.6.1. Etapas de la EIPD

La AEPD facilita un esquema que describe a la perfección las etapas que debe tener una EIPD, como se puede ver más adelante en la figura 8.

Por partes:

-El primer paso será **analizar si es necesario realizar una EIPD**, porque en el caso de que no sea necesario también hay que documentar los motivos.

-Después, se **describe el ciclo de vida de los datos,** y el flujo de datos de tratamiento. Se identifican los datos, los intervinientes, terceros, los sistemas aplicados y cualquier elemento relevante. Igual que se mostraba antes en la plantilla de la figura 6.

-En tercer lugar, se **analiza la proporcionalidad y necesidad del tratamiento,** la base de legitimación, la finalidad, proporcionalidad y necesidad del tratamiento.

-Después, se realiza la **gestión de riesgos** que incluye, **identificar riesgos y amenazas, evaluar los riesgos y tratarlos.** Para conseguir minimizar su impacto o evitarlos, así como conseguir un riesgo aceptable.

-Casi para terminar, en conclusión y validación, se hará el **plan de acción y las conclusiones.** Se dará el resultado obtenido y el plan mencionado con las medidas a implantar.

-Por último, se debe realizar una **supervisión y revisión de la implantación** de manera constante para garantizar que se implantan las medidas del plan establecido. Además, la EIPD debe ser un proceso de mejora continua y cualquier cambio que muestre una amenaza debe conllevar una nueva evaluación, un nuevo informe y un nuevo plan. En el caso de que el cambio no muestre una amenaza, se documentan igualmente con los motivos que hacen que no sea necesario implantar nuevas medidas.

2.6.2. ¿Quién debe realizar la EIPD?

Después de las etapas, hay que pasar a hablar del **responsable del tratamiento** como **actor principal para realizar la EIPD**. El encargado debe apoyar y colaborar con el primero y, además, el Delegado de Protección de Datos, a partir de ahora, DPD, no es una parte obligatoria por norma general, pero si la hay, se encarga de asesorar al responsable para el desarrollo de la EIPD.

Existen otras figuras con menor importancia pero que también pueden participar, como son: el encargado de seguridad, el área jurídica o la de tecnología, entre otros.

Por tanto, el resumen de las funciones es el siguiente:

-**Responsable:** lleva a cabo todas las etapas. Si encarga un tratamiento, debe ser el responsable de validar y llevar a cabo su ejecución.

-**Encargado:** es consultado para llevar a cabo todas las etapas.

-Delegado: igualmente, debe ser consultado para llevar a cabo las tareas y, además, debe ser informado de su realización.

3. Propuesta

Tras esta extensa explicación y puesta en contexto, llegamos al punto en el que se desarrolla el objetivo del trabajo, desarrollar una guía para la realización de la EIPD que pueda ser de ayuda para los encargados y responsables del tratamiento de datos.

Como se ha desarrollado brevemente en el punto anterior, la realización de la EIPD se compone de diferentes fases para conseguir la gestión de los riesgos. Lo más importante es tener claro cuáles son estas fases, qué objetivos y tareas se deben conseguir en cada una y quién se encargará de realizarlo.

3.1. Metodología EIPD

Por tanto, pasamos a detallar una a una las fases de ejecución de la EIPD, que son las que se pueden ver en la figura 8.

- **Analizar la necesidad de una EIPD**

Se debe empezar por el análisis preliminar, que será **analizar la necesidad de una EIPD**, es muy importante, porque el tratamiento puede no requerir EIPD, y la forma de actuar sería la comentada en el apartado de análisis de riesgos. Se debe documentar la elección tomada y los motivos que llevan a ella, tanto si debe hacerse la EIPD como si no.

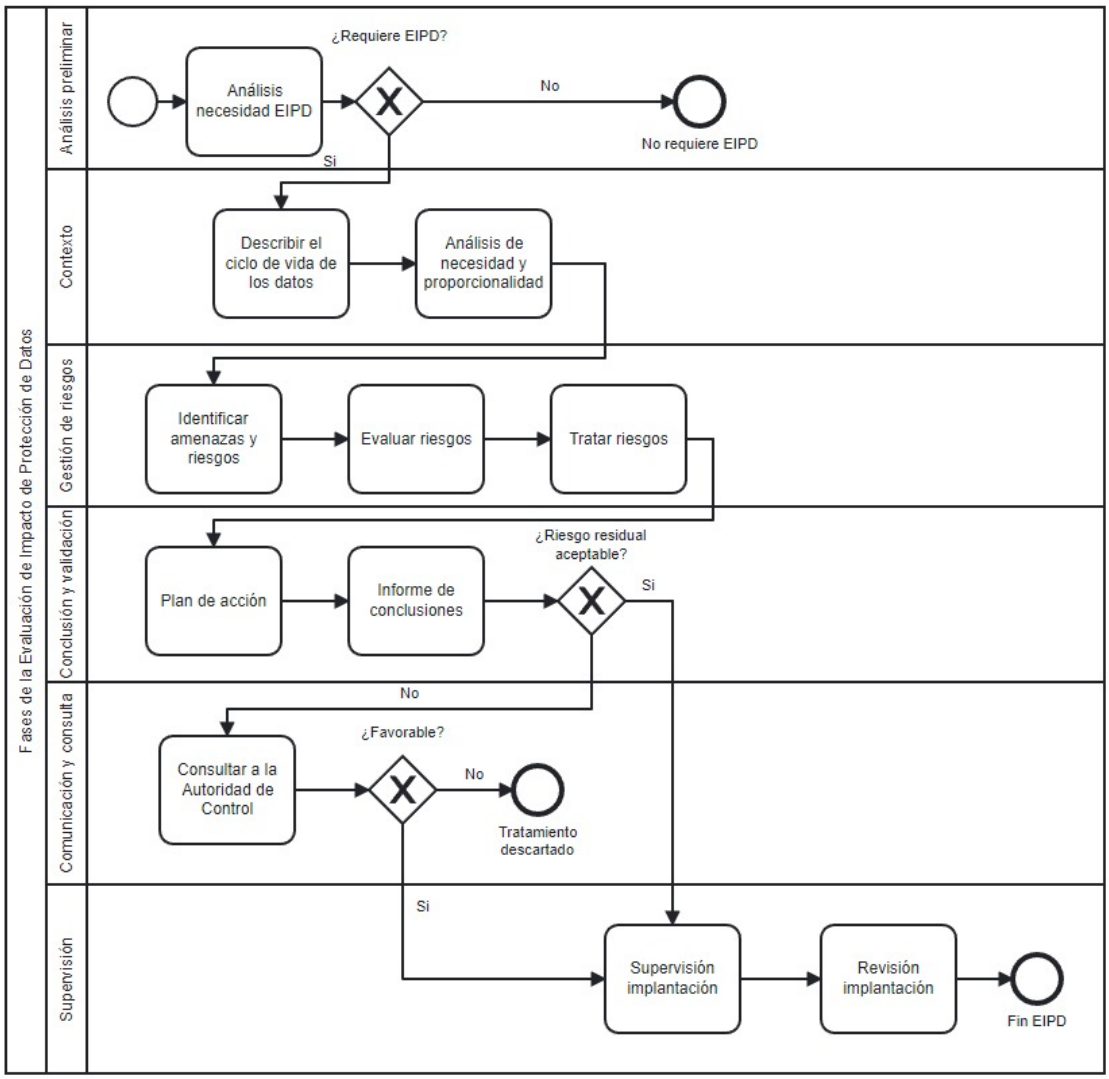

Figura 8. Fases de la EIPD

Fuente: Elaboración propia a partir de la AEPD, 2022

- **Desarrollar el ciclo de vida de los datos**

Cuando se requiere una EIPD, se pasa a las siguientes fases. Lo primero entonces es **explicar el ciclo de vida de los datos.** Se completará la tabla de la figura 6 o alguna similar, con el ciclo de vida y el flujo de los datos. En esta parte se debe incluir una descripción sistemática y detallada del tratamiento y se debe facilitar la identificación de riesgos y amenazas de los datos. Su ciclo de vida ha sido detallado tras la figura 5.

- **Analizar la proporcionalidad y necesidad del tratamiento**

El siguiente paso es **analizar la proporcionalidad y necesidad del tratamiento,** en este paso se deben revisar todas las actividades y plantearse, entre otras cosas, cuál es el fin con el que se van a tratar los datos, cuáles de los datos se van a tratar o de quién son esos datos. Además, una vez está eso claro, se debe aclarar la base legitimadora en la que está basado el tratamiento, comprobando las bases jurídicas. Los datos deben ser tratados de forma lícita, así como recoge el artículo 6 del RGPD, no se deben tratar con una finalidad diferente a la establecida. Además, se debe cumplir la "minimización de datos", es decir, incluir únicamente los estrictamente necesarios.

- **Gestión de riesgos**

Después se pasa a la parte extensa, la **gestión de riesgos que incluye tres partes: identificación, evaluación y tratamiento de riesgos.** El objetivo de este punto, como ya se ha mencionado, es minimizar el nivel de exposición al riesgo de los datos tratados.

La primera parte es **identificar las amenazas y riesgos,** en la primera fase de la EIPD se tiene información suficiente para poder identificarlos. Esta es la parte clave para la evaluación completa y correcta.

El riesgo es la exposición a las amenazas, pero, ¿Qué son las amenazas?

Las amenazas son todo tipo de factores de riesgo que puedan causar un daño en los interesados, de los cuáles se están tratando los datos. Los diferentes tipos son: desastres naturales, fallos, ataques intencionados o incumplimientos normativos, pero en la protección de datos interesan 3 tipos de amenazas:

-Las que **conllevan riesgo sobre la integridad de los datos**, como modificación no autorizada de los datos. Algunos ejemplos son: suplantaciones de identidad o modificaciones no autorizadas e intencionadas.

-Las que **conllevan riesgo sobre la disponibilidad de los datos**, como un borrado de datos. Como ejemplos se pueden poner: cortes en el suministro de electricidad o desastres naturales.

-Las que **conllevan riesgo sobre el carácter confidencial de los datos** como un acceso ilegítimo a los datos. Como acceso a datos por personal no autorizado o pérdidas de dispositivos electrónicos.

Para identificarlas, se debe tener muy en cuenta para los datos, su ciclo de vida completo e identificar cuál es el origen de los escenarios en los que se puede dar una violación de los derechos. Existen diversos catálogos con ejemplos de amenazas y, además, cada entidad puede contar con el suyo propio que le ayude a trabajar de manera más sencilla. Y, además, existen muchas preguntas que se pueden formular para identificarlas.

Por tanto, la preocupación es sobre la posible materialización de la amenaza y las consecuencias que puede traer, que serán negativas. Y para evaluar el riesgo y su impacto, se deberá saber la probabilidad de que este se materialice y el posterior impacto.

Se puede explicar todo esto con un ejemplo, en el que la amenaza podría ser un desastre natural que pueda provocar pérdida de datos, el riesgo, la falta de disponibilidad de ciertos datos para una operación del tratamiento y el impacto, los posibles daños materiales al interesado.

La segunda parte es **evaluar los riesgos,** consiste en determinar la probabilidad de que se materialice el riesgo y el impacto que podría tener. Para ello, existen varios métodos y conceptos.

Lo primero es hablar del **riesgo inherente**, que es un riesgo intrínseco que tienen las actividades sin contar con las medidas que reducen el nivel de exposición. Se calcula como "**Probabilidad X Impacto**", y para valorar estos dos, se puede utilizar una metodología que se basa en cuatro niveles, de acuerdo a la ISO 29134.

Hay dos escalas, la primera es la de los valores para el cálculo de la probabilidad, que puede ser:

-Despreciable: muy baja, un evento fortuito.

-Limitada: baja, un evento ocasional.

-Significativa: alta, un evento frecuente.

-Máxima: muy elevada, un evento muy frecuente.

Y la segunda es la misma para los impactos, según los daños que se puedan producir si la amenaza ocurre, pueden ser:

-Despreciable: muy bajo, evento con consecuencias despreciables.

-Limitado: bajo, consecuencias sin impacto

-Significativo: alto, consecuencias implican un daño elevado con impacto.

-Máximo: muy alto, daño muy elevado e impacto crítico.

El impacto produce un daño para el interesado que puede ser: daño físico, material o moral. Y de estos daños depende el tipo de impacto causado.

Y con estas dos escalas se determinará el riesgo inherente. Para ello se asignan valores del 1 al 4 a los cuatro niveles. El 1 será el despreciable y el 4 el máximo, y con esto, se forma una matriz de riesgo que se representa en la figura 9.

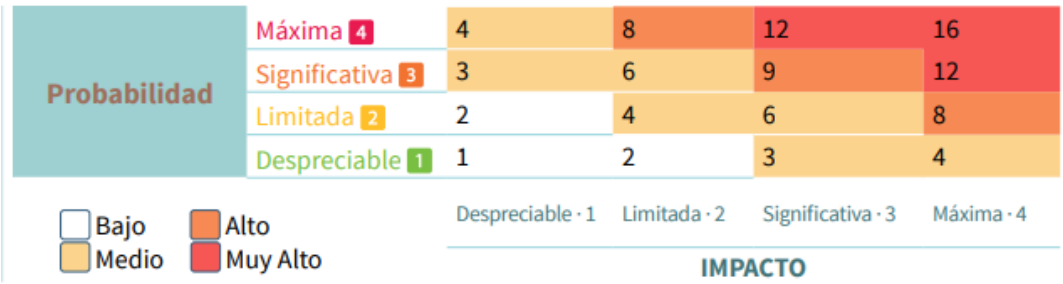

Figura 9. Matriz de riesgo

Fuente: AEPD, 2021

Se multiplican los diferentes valores para obtener el riesgo, como se ha visto en la fórmula. Y como se puede ver, se valoran los niveles según la leyenda:

-Bajo: entre 1 y 2.

-Medio: mayor de 2 y menor o igual a 6.

-Alto: mayor de 6 y menor o igual a 9.

-Muy alto: mayor de 9.

Por tanto, para cada amenaza se realizará este cálculo para saber el riesgo inherente.

Y la tercera parte de la gestión de riesgos es **su tratamiento o respuesta.** En esta etapa se debe dar la respuesta o las medidas pertinentes para tratar el riesgo y disminuir el nivel de exposición. Y para ello existen cuatro medidas diferentes:

-Reducción del riesgo: reducir los niveles de probabilidad o de impacto que tiene el riesgo inherente.

-Transferencia del riesgo: compartirlo con una organización externa, como por ejemplo una aseguradora. Pero esta transferencia puede conllevar otros riesgos.

-Retención del riesgo: en caso de que el riesgo inherente sea inferior al riesgo aceptable, no son necesarios controles adicionales.

-Anulación del riesgo: en el caso de que fuese muy elevado, se podría llegar a abandonar la actividad de tratamiento.

Estas medidas pretenden reducir o anular el riesgo de una operación de tratamiento. Aunque el objetivo de la EIPD no es eliminarlo completamente, es reducirlo al máximo hasta llegar a un nivel aceptable.

Cada riesgo se evalúa individualmente y se toman medidas para cada uno, y estas medidas son de diferentes tipos:

-Organizativas: se asocian al funcionamiento de la entidad, a procesos y organización, por ejemplo, procedimientos y protocolos para asegurar los derechos de los interesados.

-Legales: respectivas al cumplimiento normativo, como recogidas de consentimientos mediante cláusulas.

-Técnicas: las que velan por la seguridad lógica, integridad o confidencialidad de la información. Como puede ser controles de acceso o cifrados.

Y una vez aplicadas las medidas para reducir o mitigar los riesgos, se debe evaluar el **riesgo residual**, que es el resultante al aplicar estas medidas. Para evaluarlo, se estiman de nuevo el impacto y la probabilidad teniendo en cuenta las medidas y se multiplican, igual que en la fórmula del riesgo inherente.

Con esta parte se termina con la gestión de riesgos, y además, en el anexo 4 se puede observar una plantilla que podría ser utilizada para documentar el proceso descrito.

Tras esta parte, se pasa a la fase de **conclusión y validación.** En esta fase, la primera parte es elaborar un **plan de acción,** que son todas las iniciativas que se tienen que desarrollar para implantar las medidas de control que reducirán el riesgo de la actividad. El plan de acción debe incluir como mínimo:

-Control

-Descripción del mismo

-Responsable de implantación

-Plazo de implantación

Además, se deberá tener en cuenta si la EIPD se ha hecho para un tratamiento nuevo o para un tratamiento que ya existía.

Si es **nueva**: el plan de acción estará en la fase de definición de exigencias de la actividad, según el principio de privacidad desde el diseño y por defecto.

Si **ya existía**: se debe plantear un proyecto para implantar las medidas del plan, con un plazo máximo establecido por el responsable. En caso de no cumplirse el plazo, podría llegar a interrumpirse el tratamiento hasta que se implanten las medidas.

Y con esto, se realizará el **informe de conclusiones.** En el informe estará el contenido íntegro del proceso, desde identificación hasta plan de acción, las revisiones que se comentarán después, también se deben incluir en dicho informe a modo de anexos.

Si el informe es negativo, se estudiará la probabilidad de añadir más medidas de control para rebajar el riesgo. Si no, el tratamiento no se podría realizar y se tendría que iniciar el proceso de **consulta con la Autoridad de Control**.

La consulta debe incluir: las tareas de encargados y responsables, los medios y los fines del tratamiento, las medidas con las que se van a proteger los derechos, los datos de contacto del delegado si lo hay, la EIPD y toda información solicitada por dicha Autoridad.

Para la consulta anterior, la AEPD dispone de un servicio de consulta electrónica[12], que también se puede utilizar al inicio del tratamiento. Si en esta consulta se obtiene un informe favorable, se pasará a la **supervisión de la implantación,** que se comentará después. Si sigue siendo no favorable, se descarta finalmente el tratamiento.

[12] Consulta previa al inicio de tratamientos de riesgo alto https://sedeagpd.gob.es/sede-electronica-web/vistas/formConsultaPrevia/procedimientoConsultasPrevias.jsf

Por el contrario, si el informe de conclusiones es positivo y se aprueba, la actividad de tratamiento se llevará a cabo, si se asegura que las medidas de control establecidas se han implantado. Se pasará entonces a la fase de supervisión.

En el anexo 5 se puede encontrar una plantilla que servirá de ayuda para documentar el plan de acción y la conclusión de la EIPD.

Para terminar, es necesario incluir una fase de **supervisión.** Esta fase empieza por la **supervisión de la implantación** monitorizada, mencionada antes. Además, también se debe realizar una **posterior revisión post-implantación periódica** de todas las medidas adoptadas en la EIPD, para garantizar que se siguen cumpliendo las libertades y derechos de los interesados con el tiempo, que es el objetivo principal perseguido.

Con todos estos pasos y como se veía en la figura 8, se habría llegado al final de la EIPD, a no ser que sea descartada tras los informes no favorables.

3.2. Autoridades de control

Aunque al comentar la necesidad de consultar a la Autoridad de Control se ha mencionado el servicio de la AEPD, existen diversos portales de diferentes autoridades de control que disponen de herramientas software gratuitas, y estas herramientas ayudan al responsable a aplicar las medidas de responsabilidad proactiva.

1 - AEPD

La **AEPD** es la agencia principal en la que se apoya todo lo relativo a las guías para la realización de las EIPD.

Además, dispone de cuatro herramientas web:

-Facilita RGPD: únicamente la pueden utilizar empresas que trabajen con datos de riesgo escaso. La aplicación consiste en responder preguntas de formularios que va ofreciendo la web.

La web ofrecerá la documentación necesaria para cada empresa, añadiendo las cláusulas informativas y contractuales, los registros de actividades y las medidas de

seguridad que recomiende. La documentación se deberá revisar y ajustar por parte de la empresa interesada.

Podrían darse numerosos problemas si se utiliza la aplicación Facilita RGPD para analizar riesgos elevados. Un claro ejemplo es una noticia de finales del año 2021 en la que se expone un caso de mal uso de dicha herramienta.

El caso consistía en el uso de la huella dactilar de los trabajadores para su fichaje de entrada y salida al trabajo. La empresa declara que se utilizó Facilita RGPD obteniendo de la misma el resultado de "riesgo escaso" por lo que no fue necesario realizar la Evaluación. Aun así, la empresa fue sancionada con 20.000€ por parte de la AEPD, argumentando esta última que se trata de datos biométricos, que pertenecen a la categoría de datos especiales.

Tras evaluar la situación mediante la legislación vigente, y argumentando la AEPD que además de existir sistemas alternativos con los que realizar el control de forma correcta, se debería haber realizado la Evaluación de Impacto de Protección de estos Datos personales, se decide sancionar a la empresa dado que el proceso realizado no cumple con los principios del tratamiento de datos: necesidad, proporcionalidad y minimización.

-Gestiona EIPD: similar a Facilita RGPD, con formularios y una serie de preguntas, pero además de realizar análisis de riesgos, realiza la EIPD.

Al terminar el proceso, se verán los riesgos a mitigar y se podrá generar un informe de riesgos o el de la EIPD.

Ninguna de las dos almacena los datos, por lo que se debe realizar el proceso completo de una.

-Informa RGPD: en esta plataforma, los responsables, encargados y DPD pueden consultar dudas sobre aplicar el RGPD en las diferentes instituciones.

-Facilita EMPRENDE: parecida a Facilita RGPD, pero esta es orientada a startups y emprendedores, ya que incluye tecnologías novedosas y estas pueden conllevar numerosos riesgos.

Y al acabar, esta herramienta genera: registro de actividades, una hoja de registro de los incidentes para documentar las brechas de seguridad, cláusulas contractuales para la política de cookies o el contrato de tratamiento, entre otras.

-Evalúa-Riesgo RGPD: se trata de una nueva herramienta muy reciente, con el mismo fin. Ayudar a encargados y responsables a identificar riesgos para los derechos y las libertades de los interesados. La misma es capaz de hacer una primera evaluación del riesgo intrínseco, detectar la necesidad de la EIPD y estimar el riesgo residual.

2 - APDCat

La Autoridad catalana, además de ofrecer multitud de información, cuenta con la herramienta software RAT, Registro de Actividades de Tratamiento.

-RAT: Está desarrollada únicamente para sistemas Windows, es muy intuitiva y, además, trabaja sin bases de datos externas. Aunque para el usuario es mejor que las ofrecidas por la AEPD, esta solo se puede utilizar para crear, gestionar y mantener los registros de las actividades. Y, además, generar informes de los mismos.

Al contrario que la anterior, esta sí permite mantener guardados los datos e ir actualizando.

3 - CNIL

La entidad francesa cuenta desde 2021 con el software PIA, para ayudar a los responsables del tratamiento. Está disponible tanto en francés como en inglés y se puede utilizar tanto en web como en escritorio. Se trata de una interfaz amigable y didáctica para realizar la EIPD, además de una base de conocimientos legales y técnicos.

Hasta la fecha, es una de las mejores desarrolladas de todas las que se han mencionado.

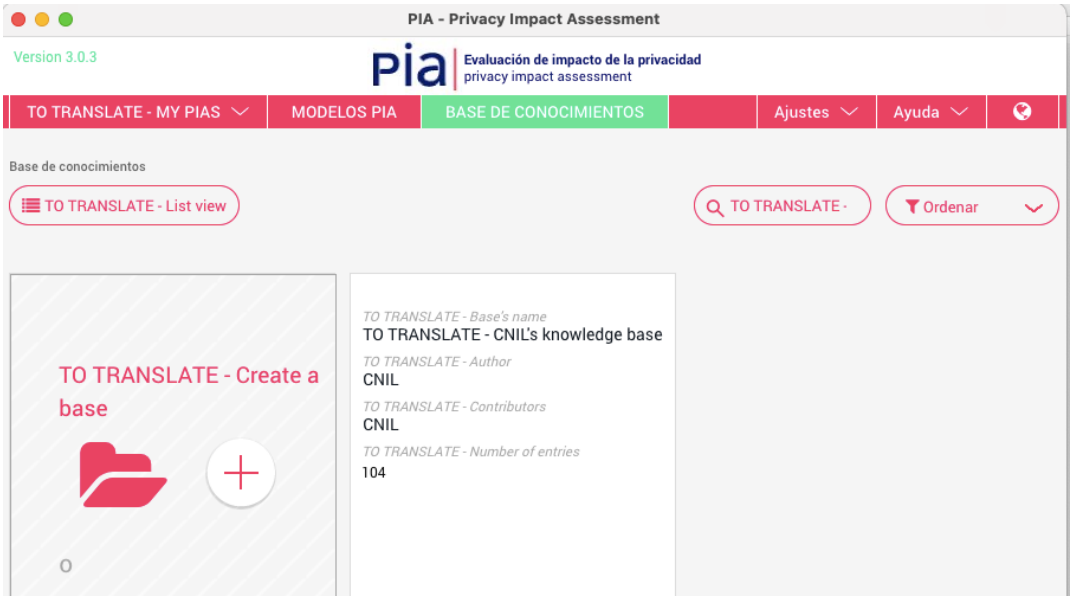

Figura 10. Interfaz aplicación PIA de CNIL

Fuente: CNIL, 202

-PIA: consiste en una guía creada para cumplir la normativa y una aplicación para poder hacer la EIPD. Además de formularios para rellenar, cuenta con una serie de conceptos del RGPD que se pueden ir mirando a la hora de realizar el formulario.

Está desarrollada sobre Electron[13], un framework (marco de desarrollo) para desarrollos con JavaScript, lo que hace que sea multilenguaje (en varios idiomas) y multiplataforma (en diferentes sistemas operativos) y además que se puedan crear aplicaciones para escritorio basadas en la tecnología web.

3.3. Aplicación Radar COVID19

Para empezar con este ejemplo, se debe introducir qué es la aplicación Radar COVID19[14], aunque seguro que cualquier lector que haya vivido la pandemia COVID habrá escuchado al menos hablar sobre ella.

[13] Web del framework Electron: https://www.electronjs.org/

[14] Aplicación Radar COVID19 https://radarcovid.gob.es/home

Es un ejemplo muy interesante ya que, su objetivo principal fue utilizar la tecnología para contener la pandemia Covid-19.

La aplicación fue desarrollada para ayudar a controlar la propagación de la pandemia identificando los posibles contactos estrechos positivos mediante Bluetooth. Los contactos estrechos son las personas que hubieran estado a menos de dos metros y más de 15 minutos en el mismo lugar que la persona que está utilizando la aplicación y la primera, notifica que es positivo en COVID.

Figura 11. Aplicación Radar COVID-19

Fuente: radarcovid.gob.es, 2020

Consiste básicamente en un rastreo de contactos para facilitar la tarea a una persona que contrae la enfermedad de avisar a todos sus contactos estrechos para ponerles en precaución.

La aplicación fue desarrollada por la Secretaría de Estado de Digitalización e Inteligencia artificial con el apoyo del Ministerio de Sanidad, unos meses más tarde del comienzo de la pandemia, aunque ha sido una aplicación con una aceptación leve.

Una vez resumido brevemente en qué consiste dicha aplicación, pasamos a hablar del Informe de EIPD realizado por el Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España aproximadamente por noviembre de 2020.

3.3.1. EIPD en la aplicación Radar COVID19

Debido al uso de datos de localización y rastreo de contactos, es necesario poner en marcha una política de protección de datos en la aplicación mencionada. Por tanto, se realizó la EIPD de la misma, que ahora se va a comentar, ya que es un ejemplo interesante en los tiempos que corren. Además, se ha elaborado siguiendo la misma plantilla que se ha utilizado para crear la guía del presente trabajo.

En este caso, los datos que recopila la aplicación no permiten identificar directamente al usuario, sólo serán los necesarios para advertirle del contacto estrecho. No se almacenará ningún dato de geolocalización.

Aunque no se pueda identificar directamente al usuario, si será posible hacerlo de una manera indirecta, además, el tratamiento de la información del usuario que utiliza la aplicación y comunica un positivo en la enfermedad, le afectará tanto a él como a sus contactos estrechos, es decir, a terceras personas.

Como ya se ha comentado a lo largo del trabajo, los tratamientos que utilizan nuevas tecnologías son más probables de producir un alto riesgo, y la aplicación mencionada las utiliza.

Además, la AEPD ofrece una lista con criterios que, si son cumplidos por la aplicación, se deberá realizar la EIPD. La aplicación se puede identificar con los siguientes supuestos:

-Tratamiento que implica uso de datos a gran escala: por el número de interesados afectados, el volumen de datos objeto de tratamiento, la duración y el alcance geográfico.

-Tratamiento que implica observación, control o supervisión del interesado de forma exhaustiva y sistemática: recogida de datos a través de la aplicación y el procesamiento de identificadores únicos para identificar a los usuarios.

-Tratamiento que hace uso de alguna categoría especial de datos: datos referentes a la salud, que son datos especiales como se ha comentado en el trabajo.

-Tratamiento que implique la utilización de nuevas tecnologías: como ya se ha mencionado, y además a gran escala. Y esta aplicación usa el Bluetooth.

-Y, además, el Comité Europeo de Protección de Datos asegura que ha de llevarse a cabo la EIPD porque se puede entrañar un alto riesgo al utilizar datos sanitarios, adopción previa a gran escala, seguimiento sistemático y utilización de una nueva solución tecnológica. Lo que se había mencionado justo antes en los criterios.

Se concluye pues, que se trata de un nivel de riesgo elevado y se debe realizar la EIPD para realizar una gestión del riesgo adecuada.

Para empezar con la EIPD, se debe saber quiénes son los responsables del tratamiento.

En este caso los **responsables** son las comunidades autónomas, Ceuta y Melilla y la Dirección General de Salud Pública, dependiente del Ministerio de Sanidad, porque deben garantizar que se cumplen las medidas de seguridad correspondientes.

El **que se encarga del tratamiento** será la Secretaría General de Administración Digital, que desarrolló la aplicación.

El tratamiento tiene como **objetivo** que las personas que hayan podido tener contacto con una persona que contraiga la enfermedad puedan ser informadas.

Los **datos personales a los que accede** la aplicación son:

-Datos de proximidad generados por la misma, con intercambio de señales por Bluetooth entre dispositivos

-Dato por el que se advierte al usuario de que es contacto estrecho y tiene riesgo

-El día en que el usuario tuvo síntomas de COVID-19

-Código que proporciona una autoridad sanitaria a un usuario para introducirlo en la aplicación cuando es positivo en la enfermedad y se pueda activar la alerta

-La dirección IP del dispositivo

Y existe el riesgo de que un usuario pudiera ser identificado y su privacidad estaría amenazada, ya que entonces quedan al descubierto multitud de sus datos personales.

Y sabiendo esto, se empezarán a seguir los pasos explicados para realizar la EIPD, que se pueden ver en la figura 8.

El primero será **describir cuál es el ciclo de vida que tienen los datos**, desde los actores hasta los elementos que intervienen en las actividades desde el principio hasta el final.

Fase	**Actividad**	**Actores**	**Sistema**
Captura de datos	Accede a la información del dispositivo al instalar la aplicación	Usuario	Dispositivo móvil
Almacenamiento	Generar códigos aleatorios		
	Compartición por Bluetooth	Usuarios	Dispositivo móvil
	Recolectar balizas de usuarios diagnosticados de COVID	Administradores de Amazon	Serv. externo: Serv de Amazon
Uso y tratamiento	Autoridad sanitaria entrega código de positivo a un usuario	Autoridad sanitaria	Servicios de Salud de cada comunidad
	Activar mecanismo de seguimiento de contactos estrechos		Servidores de AWS
Cesión	Integración con otros sistemas de la UE	Comisión Europea	Pasarela Federativa
Destrucción	Destruir la información cuando pasa el plazo legal	Usuarios	Desinstalar APP
	Detener todo tipo de recogida de información cuando se declare el fin de la pandemia	Autoridades sanitarias	

Tabla 2. Fases del ciclo de vida de la aplicación

Fuente: Elaboración propia a partir de Radar COVID Informe de EIPD, 2022

La siguiente parte es **Analizar la proporcionalidad y necesidad del tratamiento**, se deben utilizar los datos estrictamente necesarios como dice el principio de “minimización de datos”.

Es necesario determinar si es proporcional y para ello hay que asegurar los principios del **juicio de proporcionalidad:**

-Principio de limitación del objetivo final: recoger datos con los fines limitados, aunque se permite la investigación científica.

-Principio de minimización de datos: tratar únicamente los datos pertinentes.

-Principio de limitación del plazo de conservación: no guardar datos más tiempo del necesario.

Del mismo modo, hay que determinar que sea **necesaria**, y que no exista otra forma más moderada de hacerlo. Se ha visto que la legislación sectorial de materia sanitaria no tiene instrumentos precisos para la situación actual. Por tanto, se ha aprobado el desarrollo de la aplicación.

La aplicación no se puede sustituir pero se utiliza únicamente como apoyo al rastreo manual del personal sanitario. Se ha concluido que la aplicación cumple los principios de idoneidad porque consigue los objetivos que se han propuesto y los de necesidad porque no hay una alternativa que no sea tan invasiva para la privacidad.

Tras esto, se ha de pasar a la parte de **gestión de riesgos**, empezando por la **identificación de amenazas y riesgos.**

En la creación de la aplicación, se le ha dado mucha importancia a la “Privacidad desde el diseño y por defecto”, porque se asegura la privacidad desde código y diseño. Y se crea de forma que se asegura que la información no llega a terceros. Y también se ha dado mucha importancia al principio de minimización de datos, como se ha comentado, los datos necesarios son los imprescindibles, como por ejemplo, no requerir la ubicación del usuario, y se almacenan durante el tiempo mínimo que establecen los protocolos.

Se da mucha importancia a la no identificación del usuario, debido al tema que se trata: datos de salud, en concreto, contagios de la enfermedad COVID. Por tanto, dados los principios de integridad y confidencialidad, se decide aplicar medidas organizativas y técnicas para asegurar un nivel de seguridad alto. Se aplica: pseudonimización, cifrado,

acuerdos de confidencialidad, distribución estricta de roles de acceso y establecimiento de restricciones y registros de acceso.

La segunda parte de la gestión será **evaluar los riesgos.** Aunque en este caso, ha sido realizado con una herramienta del CCN-CERT: PILAR[15]. En la misma, se han realizado múltiples actividades:

-Caracterización de activos: identificación y valoración de activos.

-Caracterización de amenazas: identificar amenazas sobre cada activo de información, la frecuencia en la que aparecen y el daño que pueden hacer. Y con toda la información se consigue determinar el **Riesgo Potencial**.

Y algunas de las amenazas identificadas son:

-Suplantación de identidad

-Abuso de privilegios de acceso

-No tramitar sobre el interesado el ejercicio de sus derechos

-Tratar datos excesivos para la finalidad

-Transferir a países a nivel internacional que no ofrezcan un nivel de seguridad y protección adecuado.

Estas amenazas se acompañan de un nivel de ocurrencia y un nivel de degradación. Se puede observar este proceso completo y visualizar todas las amenazas en el documento "Radar COVID, Análisis de riesgos"[16]. Y gracias a estos niveles, se consigue una estimación del riesgo potencial de cada activo. En la siguiente tabla, se puede ver de manera resumida el riesgo potencial de cada activo de esta aplicación.

Activo	**Riesgo potencial**
Servicio Radar Covid	6.3
Teléfono Móvil	2.7

[15] Herramienta PILAR: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/10388-nuevo-portal-de-pilar-la-solucion-de-analisis-y-gestion-de-riesgos-del-ccn.html

[16] Análisis de riesgos Radar COVID https://raw.githubusercontent.com/RadarCOVID/radar-covid-documentation/7fc407f52010e9fa7a216ba6c2b1ddad293ba51d/AARR.pdf

Redes de Comunicaciones	5.3
App Radar Covid19	5.1
Administradores / Operadores	4.8
Desarrollo y Mantenimiento de la App	4.2
Desarrolladores	4.2
Ciudadanos	3.7
Soportes	5.7
Instalaciones AWS	5.1
Equipos AWS	5.1
Repositorio Descargas Apple	4.2
Servicio Cloud	4.2
Repositorio Descargas Android	4.2

Tabla 3. Riesgo potencial activos

Fuente: Elaboración propia a partir de Radar COVID Informe de EIPD, 2022

Y tras detectar los riesgos potenciales, se debe pasar a la última parte de la gestión, **el tratamiento de los riesgos.** Con el objetivo de reducirlos al máximo o mitigarlos, como se ha explicado previamente. Se va a reducir el riesgo mediante salvaguardas, mecanismos tecnológicos que lo consiguen. De esta forma se consigue que los riesgos sean prácticamente inexistentes, y se mitigan las amenazas.

Y después, para valorar la eficacia de las medidas aplicadas, utilizan el "Modelo de Madurez de la Capacidad".

Y tras la gestión, se debe repetir la tabla 3 pero esta vez, con el riesgo residual, tras las medidas. Se muestra a continuación:

Activo	**Riesgo potencial**
Servicio Radar Covid	2.6
Teléfono Móvil	0.47

Redes de Comunicaciones	0.97
App Radar Covid19	0.91
Administradores / Operadores	0.81
Desarrollo y Mantenimiento de la App	0.69
Desarrolladores	0.83
Ciudadanos	0.58
Soportes	1
Instalaciones AWS	0.96
Equipos AWS	0.95
Repositorio Descargas Apple	0.83
Servicio Cloud	0.83
Repositorio Descargas Android	0.83

Tabla 4. Riesgo residual activos

Fuente: Elaboración propia a partir de Radar COVID Informe de EIPD, 2022

Tras esto, se llega al **plan de acción** para tratar los riesgos, en la parte de **conclusión y validación.** Se busca conseguir que todos los riesgos estén por debajo del nivel Medio, cuyo valor es entre 2 y 6.

El único activo en este rango es el de Servicio Radar Covid19, se identifican y aplican salvaguardas sobre este para conseguir que llegue a un Riesgo Objetivo de 1.8, suficiente para seguir adelante con el tratamiento.

Quedan entonces tras la evaluación completa, 12 activos con riesgo despreciable y 2 con riesgo bajo.

Y con esto, terminaría la investigación sobre la EIPD de la aplicación Radar Covid19, concluyendo que **se puede realizar el tratamiento** si se aplican las medidas de seguridad y el plan de acción desarrollados.

4. Conclusión

Si el lector se remonta a la introducción, recordará la importancia de vigilar a quién y para qué se ceden los datos y de leer detenidamente qué letra pequeña se acepta, sobre todo cuando los datos personales resultan implicados. Como se ha podido ver, se trata de un tema que debe proporcionar gran seguridad y del cuál los ciudadanos, por suerte, están amparados gracias a la legislación referente de protección de datos vista.

En 2020, en Netflix se hizo muy viral un documental llamado: "*El dilema de las redes sociales*"[17]. Este documental habla sobre la peligrosa influencia que tienen las redes sociales y las plataformas en las que se introducen los datos. Se puede escuchar a numerosos profesionales y expertos del ámbito, por lo que, llegados a este punto del trabajo y si el tema le ha resultado de interés, se recomienda este documental al lector.

En el presente trabajo, se proponían inicialmente diferentes objetivos, el principal de ellos, crear una guía para ayudar a los responsables del tratamiento de datos personales, al realizar la EIPD. Todo ello además, respetando la normativa. Una vez finalizado este trabajo, se considera prácticamente alcanzado el objetivo principal, habiendo presentado una guía práctica y ejemplificada que puede llegar a resultar de ayuda a los encargados y responsables. Sobre todo si se estudia en profundidad, dado el contenido de la misma en legislación e información proporcionada por la Agencia Española de Protección de Datos, que se ha intentado sintetizar.

Además del objetivo principal, se propusieron diferentes objetivos específicos. En cuanto a "Analizar el contenido del nuevo reglamento", se han dedicado unos apartados en "Estado del Arte" al mismo tema, actualidad en la ley y novedades legislativas, que desde 2018 se ha visto que es el RGPD junto a la LOPDGDD.

Por la entrada en vigor del RGPD en 2018, se ha podido comprobar la importancia que se le ha tenido que dar a los temas tratados en el presente trabajo: Evaluar el Impacto

[17] El dilema de las redes sociales, Netflix https://www.netflix.com/watch/81254224?trackId=13752289&tctx=0%2C0%2Ccf993f3172076ae30f0ef4b559a8d41b1262b246%3A199f706210dd58bacb6801179c85e08137a71310%2Ccf993f3172076ae30f0ef4b559a8d41b1262b246%3A199f706210dd58bacb6801179c85e08137a71310%2C%2C

de la Protección de Datos y responsabilidad proactiva de todo responsable de datos. Se han encontrado numerosos trabajos realizados sobre el tema y plataformas que desde las novedades de la legislación han intentado informar sobre este tema.

Sobre “Conocer guías y herramientas proporcionadas por autoridades de control”, en el apartado 3.2. , se enumeran cada una de las más conocidas y sus formas de trabajar.

Se ha podido comprobar que debido a la reciente actualización, son muchas las agencias y plataformas que intentan ofrecer servicios pero que todavía parecen estar en desarrollo. Y además, que tanto ciudadanos como responsables, no llegan a ser conscientes al 100% de la importancia que tiene este tema.

En cuanto a “Aprender a realizar una correcta gestión de los riesgos”, se detalla en profundidad en el apartado 2.4, dicha gestión. Dando hincapié a cada una de las 3 fases de la misma: identificación, evaluación y tratamiento.

En cuanto a “Proporcionar las pautas recomendadas por las instituciones para adaptarse al RGPD”, se han enumerado las diez pautas que expone la AEPD, dando detalle en cada una de ellas.

Y finalmente, a modo de “Ejemplificación”, se ha presentado un ejemplo sobre una evaluación reciente y que en su momento álgido tocaba bastante de cerca al ciudadano. Se trata de la aplicación Radar Covid19, que ayuda a controlar los focos de contagio. Se ha explicado la EIPD realizada para la aplicación, unos meses más tarde de su puesta en marcha, y se ha podido comprobar su resultado positivo, tras tener muy en cuenta las directrices explicadas en el presente trabajo y además, imponer varias medidas de seguridad en salvaguardas.

Con lo que se puede concluir respecto a objetivos, que el trabajo ha cumplido con lo que en un principio se propuso, entre otras cosas que hayan podido ser añadidas sobre la marcha del mismo.

Personalmente, las motivaciones que inicialmente me hicieron elegir el trabajo, y que se comentaban al inicio, se han visto incrementadas al poder leer numerosa información sobre el tema. El trabajo me ha hecho pensar y recapacitar sobre todo el tema de los datos personales. Dándome cuenta que al haber iniciado el trabajo, cada vez me fijaba

más en todo lo relacionado con la protección de datos, guarda enlaces e información que pensaba podría servirme para mi trabajo.

Incluso en mi trabajo, relacionado con un ERP, en el que formo parte del equipo de finanzas, llegué a detectar ocasiones en las que la protección de datos era de gran importancia y recolectaba ejemplos que forman parte de este trabajo.

Aun así, el único punto negativo que saco del trabajo, es la cantidad de información repetida y trabajos en torno al tema que lo rodea, las guías. Esto hace que sea muy difícil realizar un trabajo como el que elegí en su momento junto a mi profesor, ya que todo lo que se debe introducir, explicar e investigar en torno al tema, se encuentra muy estudiado. Quizá, si hubiese hecho una búsqueda en profundidad, como la que hice durante el trabajo, antes de escogerlo, hubiese enfocado de otra manera el tema, por ejemplo, con el desarrollo de una herramienta.

Ya que, por el contrario, he podido ver que falta por informar y desarrollar otros enfoques, como herramientas prácticas, software, guías interactivas, otras más completas de alto nivel tanto para responsables como para ciudadanos, para que estos puedan saber qué es lo que se está haciendo en el tratamiento de sus datos. Pero como ya he dicho, esto podría haber sido otro enfoque.

Por tanto, y como evoluciones a mi trabajo o como consejo en trabajos similares, me gustaría motivar al lector, que se plantee tanto realizar una EIPD al completo, sobre algún otro trabajo, start-up, idea, etc, que pueda necesitar del mismo, si su idea es un trabajo más teórico. O como ya he mencionado, otro tipo de trabajos más relacionadas con programación y código, en el que se desarrolle una herramienta, del estilo de las existentes.

“La manera en que la tecnología funciona, no es una ley de la física. Son decisiones tomadas por seres humanos, y los seres humanos podemos cambiar esas tecnologías.” El dilema de las redes

5. 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: mayo 2022]

Agencia Española de Protección de Datos. (2021). *Evalúa-Riesgo RGPD.* Disponible en:

https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd [Consulta: mayo 2022]

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/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf-0 [Consulta: julio 2022]

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/guiamodelo-clausula-informativa.pdf [Consulta: junio 2022]

Agencia Española de Protección de Datos. (2018). *Guía para la notificación de brechas de datos personales.* Disponible en:

https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf [Consulta: abril 2022]

Agencia Española de Protección de Datos. (2018). *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: junio 2022]

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: junio 2022]

Agencia Española de Protección de Datos. (2021). *Historia.* Disponible en:

https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia [Consulta: mayo 2022]

Agencia Española de Protección de Datos. (2022). *La AEPD alcanza el 89% de cumplimiento en los compromisos adquiridos en su Plan de Responsabilidad Social 2019-2024.* Disponible en:

https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-alcanza-89-cumplimiento-en-compromiso-plan-responsabilidad-social-2019-2024 [Consulta: agosto 2022]

Agencia Española de Protección de Datos. (2022). *Memoria de responsabilidad social 2021.* Disponible en:

https://www.aepd.es/es/documento/memoria-responsabilidad-social-aepd-2021.pdf [Consulta: agosto 2022]

Agencia Española de Protección de Datos. (2021). *Persona Delegada en protección de datos.* Disponible en:

https://ayudaleyprotecciondatos.es/2020/11/19/esquema-nacional-de-seguridad-ens/ [Consulta: julio 2022]

Ayuda Ley Protección de Datos. (2020). *Esquema Nacional de Seguridad (ENS) Definición y fases.* Disponible en:

https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/persona-delegada-en-proteccion-de [Consulta: mayo 2022]

Casal Tavasci, Javier. (2018). *Los orígenes del actual marco normativo.* Disponible en:

https://protecciondata.es/un-poco-de-historia-los-origenes-de-la-actual-normativa/ [Consulta: abril 2022]

CNIL.fr. (30 de junio de 2021). *The open source PIA software helps to carry out data protection impact assessment.* Disponible en:

https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment [Consulta: julio 2022]

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 2022].

De La Higuera, Ana. (2018). *La importancia de los Privacy Impact Assessment (PIA) en la protección de datos*. KPMG Tendencias. Disponible en:

https://www.tendencias.kpmg.es/2018/01/la-importancia-de-los-privacy-impact-assessment-pia-en-la-proteccion-de-datos/ [Consulta: junio 2022]

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 2022].

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: abril 2022].

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 2022].

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: abril 2022].

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: abril 2022].

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: abril 2022]

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: abril 2022].

Galán, Dr. Carlos. (2020). *RGPD y ENS: dos caminos convergentes.* CNN-CERT. Ciberseguridad. Disponible en:

https://www.ccn-cert.cni.es/pdf/documentos-publicos/xii-jornadas-stic-ccn-cert/3434-m32-02-rgpd-y-ens/file.html [Consulta: julio 2022]

Gil Sanchidrián, Laura. (13 de diciembre de 2021). *La importancia de realizar una EIPD ante la instalación de un sistema de huella dactilar.* PRODAT. Lideres en protección de datos. Disponible en:

https://www.prodat.es/blog/la-importancia-de-realizar-una-eipd-ante-la-instalacion-de-un-sistema-de-huella-dactilar/ [Consulta: julio 2022]

Gobierno de España. (2021). *FAQS Utilizando las últimas tecnologías para contener la pandemia COVID-19.* Disponible en:

https://radar-resources.s3-eu-west-1.amazonaws.com/documento-APP-RadarCOVID-v4.pdf [Consulta: junio 2022]

Gobierno de España. (2021). *Protégete y protege a los tuyos*. Aplicación Radar COVID19. Disponible en:

https://radarcovid.gob.es/home [Consulta: julio 2022]

Gobierno de España. (4 de noviembre de 2020). *Radar COVID Informe de Evaluación de Impacto relativa a la Protección de Datos.* Disponible en:

https://raw.githubusercontent.com/RadarCOVID/radar-covid-documentation/main/EIPD.pdf

[Consulta: julio 2022]

Kemp, Simon. (26 de enero de 2022). *DIGITAL 2022: GLOBAL OVERVIEW REPORT.* DataReportal. Disponible en:

https://datareportal.com/reports/digital-2022-global-overview-report Consulta: abril 2022]

Rodríguez Ferrer, Marc. (2020). *Guía para la evaluación de impacto requerida en el Reglamento Europeo de Protección de Datos.* En: Riunet. Disponible en:

https://m.riunet.upv.es/bitstream/handle/10251/151243/Rodr%C3%ADguez%20-%20Gu%C3%ADa%20para%20la%20evaluaci%C3%B3n%20de%20impacto%20requerida%20en%20el%20Reglamento%20Europeo%20de%20Protecci%C3%B3n%20d....pdf?sequence=1&isAllowed=y

[Consulta: julio 2022]

VerificaRTVE. (14 de mayo de 2021). *Privacidad y WhatsApp: qué cambia el 15 de mayo*. rtve. Disponible en:

https://www.rtve.es/noticias/20210514/privacidad-whatsapp-cambia-15-mayo/2090420.shtml [Consulta: junio 2022]

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/legalcontent/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES [Consulta: abril 2022].

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)* Disponible en:

https://www.boe.es/doue/2016/119/L00001-00088.pdf [Consulta: abril 2022]

6. Anexos

6.1. Plantilla para el registro de actividades de tratamiento orientada el responsable

Datos comunes a todos los tratamientos

Responsable del tratamiento: Nombre y datos de contacto

Delegado de Protección de Datos: Nombre y datos de contacto

Actividad tratamiento	Finalidad	Categorías de interesados	Categorías datos personales	Cesiones de datos	Transferencias internacionales

Periodo de conservación	Medidas de seguridad

Elaboración propia a partir de la AEPD

6.2. Plantilla para el registro de actividades de tratamiento orientada el encargado

Datos comunes a todos los tratamientos

Encargado del tratamiento: Nombre y datos de contacto

Delegado de Protección de Datos: Nombre y datos de contacto

Responsable del tratamiento	Categoría del tratamiento	Transferencia de datos personales	Medidas de seguridad

Elaboración propia a partir de la AEPD

6.3. Plantilla para la redacción del análisis de riesgos básico

Gestión de riesgos por defecto

Operaciones de tratamiento:

Riesgos por defecto

	Tipología de riesgo	**Riesgos**	**Medidas de control**
Protección de los datos personales			
Derechos y libertades de los interesados			

Elaboración propia a partir de la AEPD

6.4. Plantilla de gestión de los riesgos

Gestión de riesgos

Identificación de amenazas

Referencia de la actividades del tratamiento fuente del riesgo	Operación de tratamiento	Referencia de amenaza	Amenazas	Descripción amenaza

Valoración del riesgo inherente

Referencia amenaza	Riesgo	Evaluación probabilidad (1-4)	Evaluación impacto (1-4)	Evaluación riesgo inherente	Valoración riesgo inherente

Incluir un del Gráfico del riesgo inherente

Identificación de medidas de control

Amenaza	Riesgo	Medida de control	Descripción de la medida de control	Evaluación probabilidad (1-4)

Evaluación impacto (1-4)	Evaluación riesgo residual	Valoración riesgo residual

Incluir el Gráfico del riesgo residual

Elaboración propia a partir de la AEPD

6.5. Plantilla del Plan de Acción y conclusión de la EIPD

Plan de acción

Identificación de medidas mitigantes planificadas

Referencia Amenaza /Riesgo	Referencia medida de control	Descripción de la medida de control	Responsable de la implantación	Fecha prevista	Estado actual

Elaboración propia a partir de la AEPD

6.6. Objetivos de Desarrollo Sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				**X**
ODS 2. **Hambre cero.**				**X**

ODS 3. **Salud y bienestar.**			X	
ODS 4. **Educación de calidad.**		X		
ODS 5. **Igualdad de género.**	X			
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**				X
ODS 8. **Trabajo decente y crecimiento económico.**			X	
ODS 9. **Industria, innovación e infraestructuras.**				X
ODS 10. **Reducción de las desigualdades**.		X		
ODS 11. **Ciudades y comunidades sostenibles**.				X
ODS 12. **Producción y consumo responsables.**				X
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**	X			
ODS 17. **Alianzas para lograr objetivos.**	X			

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Tras su lectura del trabajo de fin de grado referente a la Guía para la Evaluación de Impacto de la Protección de Datos, habrá podido ver la importancia de las raíces que guían todo el trabajo: la Protección de Datos Personales, y en concreto, el Reglamento General de Protección de Datos, RGPD y la Agencia Española de Protección de Datos, la AEPD.

Al estar la protección de datos personales regida por la Agencia Española de Protección de Datos, toda relación del trabajo con los Objetivos de Desarrollo Sostenible, se basa principalmente en la relación de la AEPD con los mismos.

Los 17 ODS, forman junto a las 169 metas, la Agenda 2030, que se crea en su momento para acabar con la pobreza, con las desigualdades, para promover la prosperidad y para proteger el medio ambiente, en un plazo hasta 2030.

Tras investigar sobre los Objetivos de Desarrollo Sostenible, se ha podido ver como en la puesta en marcha de los mismos a nivel mundial, todos los actores y líderes del planeta tuvieron que adaptarse y cumplir los mismos, la AEPD como organismo público, no podía quedarse atrás, y no lo hizo.

La AEPD queda enmarcada desde 2019 en un Marco de Actuación de Responsabilidad Social, dando respuesta a la Agenda 2030 mencionada, y por consiguiente, a los 17 Objetivos de Desarrollo Sostenible. La AEPD alegó en ese momento haberse sumado a la Agenda 2030 para aportar las capacidades, competencias, peculiaridades y responsabilidades que la representan.

Es por ello que en ese mismo momento, la AEPD se comprometió al cumplimiento de los Objetivos que le fuesen posibles con sus procesos y actividades, para así ser una parte de impulso clave para los ODS. Para ello emprendió 100 acciones de las cuales el 70% corresponden a compromisos de la sociedad, el 13% a compromisos internos con los empleados, el 10% están relacionadas con el medio ambiente y el 7% con un buen gobierno y transparencia.

El punto principal de las acciones tomadas por la AEPD, que se relaciona directamente con el trabajo, es la "*Prevención para una protección eficaz de los derechos de los ciudadanos*", en el que se incluyen actuaciones para los ciudadanos en general, para menores y el ámbito educativo, contra el delito en redes sociales, de colaboración con organizaciones, con medios de comunicación, herramientas y guías para impulsar el derecho de privacidad.

Para evaluar los riesgos a los que se exponen los datos al tratarlos, se utiliza la mencionada Evaluación de Impacto de la Protección de Datos referente al tratamiento de los datos de los ciudadanos, entre muchos otros. Este punto se ha podido ver claramente desarrollado en el trabajo.

Concretamente el punto 1.5 de estas acciones se denomina: "*Colaboración en guías y herramientas para impulsar el derecho a la privacidad*", la AEPD argumenta como una de las acciones, difundir guías específicas orientadas a la protección del derecho a la

privacidad y a impulsar los derechos humanos, entre las que se encontraría el presente trabajo: la "**Guía para la realización del Privacy Impact Assessment (Evaluación de Impacto en la Protección de Datos Personales) para encargados y responsables de tratamiento de datos"**.

Tras ver de qué forma se implica la AEPD con los Objetivos, mediante estas acciones, la relación del trabajo con los mismos es clara, ahora falta detallar cuáles de estos objetivos son a los que se dedica especial atención.

Según la memoria de Responsabilidad Social de 2021 de la AEPD, concretamente son el número 5: Igualdad entre géneros y empoderamiento a todas las mujeres y niñas, el número 16: Promover sociedades justas, pacíficas e inclusivas y el número 17: Alianza mundial para el desarrollo sostenible. Todo esto aplicando las respectivas medidas, según los casos.

Para el ODS 5, la AEPD plantea un Plan de igualdad interno, que pretende conseguir igualdad de trato entre hombres y mujeres, eliminando la discriminación por sexo. Para ello se compromete a alcanzar un 50% de representación femenina en sus puestos superiores, llegando a final de año a un 48,67%

Para el ODS 16, la AEPD asegura un acceso público a la información sobre protección de datos, así como proteger las libertades y la privacidad de los ciudadanos.

Y para el ODS 17, la AEPD se implica de manera plena destinando grandes esfuerzos para promover alianzas con responsables privados, públicos y demás colectivos de la sociedad. Se establecen colaboraciones con instituciones de otros países, como por ejemplo la Red Iberoamerica de Protección de Datos.
Además de todo ello, la AEPD alude seguir trabajando en guías y herramientas de apoyo a los ciudadanos y a los que tratan los datos de estos. Concretamente, 13 en 2021 y 97 desde 2015.

Por último, y para cerrar esta reflexión, es interesante el dato que anuncía la AEPD en junio de 2022. Se cumple a esa misma feche, el cumplimiento de casi el 90% de los compromisos que fueron adquiridos en el mencionado Plan de Responsabilidad Social

de 2019, respecto al ejercicio de 2021, publicando el trabajo que se ha hecho para lograrlo.