UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guía el cumplimiento de la normativa relativa a protección de datos en pequeños comercios .

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Culla de Moya, José Antonio

Tutor/a: Oltra Gutiérrez, Juan Vicente

Director/a Experimental: Fort Palau, César Martín

CURSO ACADÉMICO: 2024/2025

Resumen

La introducción del Reglamento General de Protección de Datos ha supuesto un antes y un después en el marco regulatorio a nivel europeo. Uno de los aspectos más relevantes de esta normativa es que se aplica a cualquiera que trate datos personales de terceros. Las pequeñas y medianas empresas en general, y el pequeño comercio en particular, se han visto directamente afectados por esta norma. Lo que, sumado a la escasez de recursos económicos que los caracteriza, ha supuesto que el riesgo regulatorio al que se enfrentan haya aumentado significativamente. En este trabajo se desarrolla una solución para ayudar a estos comercios a alcanzar el cumplimiento de la regulación. Para ello, se realiza un análisis de los esfuerzos previos en la materia en el que se identifican las lagunas más importantes, como son: la falta de conocimiento, la falta de recursos económicos y la falta de recursos formativos y de apoyo centrados en la creación de evidencias que puedan ser aportadas en procesos de inspección. Un negocio que cumpla con todos los requisitos de la norma, pero no puede demostrarlo será sometido a sanciones. La solución propuesta se basa en la construcción de un sistema de gestión similar a los propuestos por las normas ISO, pero adaptado a la normativa de protección de datos y, en particular, al pequeño comercio. No obstante, desarrollar un sistema de gestión adaptado no serviría de mucho por sí solo. Para evitar esto último, se implanta el sistema desarrollado sobre una serie de empresas ficticias. Estos ejemplos aportan certidumbre sobre cómo afrontar casos concretos y ayudan a lidiar con los problemas que pueden ocurrir en el día a día. Este proceso, junto con la metodología de prueba también desarrollada, permitirá al pequeño comercio evaluar la efectividad del sistema tras la implantación.

Palabras clave: protección de datos personales, pequeño comercio, digitalización, cumplimiento normativo, privacidad, guía de cumplimiento.

Abstract

The introduction of Europe's Data Privacy Act has shaken the foundation of the regulatory framework on privacy standards for Europe. The key element of this new regulation is that any entity involved in working with personal identifiable information of a natural person must adhere to new standards. Small and medium size businesses, in particular, mom-and-pop shops have been hit hard by the introduction of this brand new regulation. These kinds of businesses usually lack the necessary resources to deal with such big changes in a timely manner increasing the regulatory risk to which they're exposed. This work aims to develop a solution to help this type of businesses achieve compliance with the General Data Protection Regulation. To do so we start by analyzing the efforts brought forth by other parties in the past. As a result, we identified some of the blind spots that make this task difficult such as lack of knowledge, lack of monetary resources, lack of teaching material and resources focused on the creation of evidence that can be used as proof while facing audits. A business that complies with every requisite set forth by laws but can't prove it during an audit will face sanctions. Our solution proposes the development of a management system designed after those proposed by ISO standards but focused on data privacy regulations and specially crafted for mom-and-pop shops. However, developing such system would not do much on its own unless it includes a guide on how to use it. Because of that we also develop a series of scenarios that are applied over a few fictional companies. These examples should allow the reader to better understand how to use our solution and reduce the ambiguity of some procedures. Finally, we also include a test and improvement process to help with assessing the state of the system and improve it as time goes by.

Palabras clave: data privacy, mom-and-pop shop, small business, legal framework, compliance, privacy, guide to compliance

Resum

La introducció del Reglament General de Protecció de Dades ha marcat un abans y un després al marc regulatori a nivell europeu. U dels aspectes mes rellevants d'aquesta normativa es que es aplicable a qualsevol que tracte dades personals de tercers. Les xicotetes y mitjanes empreses en general, y el xicotet comerç en particular, s'han vist directament afectats per aquesta norma. Tot allò, sumat a l'escassesa de de recursos econòmics que els caracteritza, ha suposat que el risc regulatori al que s'enfronten haja augmentat de manera significativa. A aquest treball es desenvolupa una solució per ajudar aquests negocis a complir amb la regulació. Per això, es realitza una anàlisi del esforços previs a la matèria identificant alguns del buits mes importants com: la falta de coneixement, la falta de recursos econòmics i la falta de recursos formatius i de suport centrants a la creació d'evidències que pugen ser proporcionats als processos d'inspecció. Un negoci que compleix amb tots els requisits regulatoris, però no pot demostrar-ho s'enfrontarà a sancions. La solució proposada esta basada a la construcció d'un sistema de gestió similar als proposat per les normes ISO, però adaptat a la normativa de protecció dades y, en particular, al xicotet comerç. No obstant, desenvolupar un sistema de gestió adapta no seria de molta ajuda per si mateix. Per a evitar este problema, implantarem el sistema de gestió desenvolupat a una sèrie d'empreses fictícies. Aquests exemples aporten certesa sobre com afrontar casos particulars i ajuden a lidiar amb el problemes que poden sorgir al dia a dia. Aquest procés, junt amb la metodologia de prova desenvolupada, permetrà al xicotet comerç avaluar l'efectivitat del sistema després d'implantació.

Paraules clau: protecció de dades personals, xicotet comerç, digitalització, compliment normatiu, privacitat, guia de compliment.

Tabla de contenido

Índice de figuras

Índice de tablas

1 Introducción

Los derechos fundamentales son la base sobre la que se ha desarrollado la prosperidad de las sociedades occidentales. Estos derechos son determinantes para el establecimiento de un marco sólido sobre el que los individuos puedan desarrollar sus proyectos de vida y mejorar su estatus socioeconómico. Sin embargo, es necesaria una defensa constante de estos para que los repetidos intentos de revertir los derechos descubiertos y formalizados a lo largo de la historia no sean fructíferos. Muchos de estos derechos han sido integrados en la cultura y la tradición de la sociedad, de tal manera, que aquellos que pretenden revocarlos son considerados parias. Esto ocurre con los derechos más antiguos y asentados, por lo general, una gran parte del código penal, por ejemplo, el derecho a la vida. Nadie discute que ningún ser humano puede arrebatar la vida a otro. Por el contrario, otros derechos de desarrollo más reciente, como el derecho a la protección de los datos personales, no gozan del mismo estatus en la sociedad, hasta el punto de que muchos ciudadanos desconocen la existencia de tal derecho y lo ven como una normativa impuesta por la burocracia europea.

El derecho a la protección de los datos de carácter personal es un derecho fundamental bastante reciente en comparación con otros derechos fundamentales establecidos a lo largo de nuestra historia. Los orígenes del derecho a la protección de datos personales se remontan al derecho común anglosajón, en concreto, podemos encontrar las primeras referencias en el artículo "*The Right to Privacy*" (1) en 1890, mientras que en términos históricos podemos retrotraer su origen al aforismo inglés "*a man's house is his castle*" (la casa de cada uno es su castillo) de William Pitten. Aunque fue principalmente durante el siglo XX cuando estas ideas comenzaron a entrar en la jurisprudencia de los tribunales estadounidenses. De esta forma, el derecho a la protección de datos personales se ha desarrollado como una extensión del derecho a la intimidad y a la inviolabilidad del domicilio. Este desarrollo entiende que nuestros datos personales son parte de nuestra identidad como individuos y, como tal, deben gozar del mismo grado de protección. No fue hasta mediados del siglo XX que estas ideas dieron el salto a Europa. El Reino Unido introduce en 1967 un proyecto de ley para la protección de la privacidad que, aunque fracasa, culmina con la aprobación de la "*Data Privacy Act*" en 1982. También podemos encontrar procesos paralelos en Alemania, que pese a entrar más tarde en el debate, adelanta a Reino Unido con la aprobación de la primera ley federal en 1977 (2).

Podemos encontrar ejemplos más recientes y cercanos en la legislación española, el primero de ellos en la Constitución Española de 1978, en concreto, su artículo 18.4 establece «*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»* (3). Que adopta esa definición de la protección de datos como extensión del derecho a la intimidad del individuo. En el marco jurídico español también podemos encontrar la Ley Orgánica de Protección de Datos de 1999 (4). Este derecho se incluyó en la creación de la Unión Europea en el artículo 8 de la carta de derechos fundamentales (5) y en el artículo 16 de los tratados de funcionamiento (6). Estos derechos se formalizaron por primera vez mediante la directiva 95/46/CE (7) y, más recientemente en el Reglamento General de Protección de Datos (8), que se adapta al reglamento jurídico español mediante la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales(9).

La introducción del Reglamento General de Protección de Datos en 2016 (8) pretende establecer un marco normativo garantista para la protección de este derecho fundamental. Sin embargo, la mera creación de un marco normativo no es suficiente, debe implantarse en todos los estratos de la sociedad para que su objetivo principal pueda verse cumplido. Desde su entrada en vigor en 2018, hemos podido ser testigos de las dificultades que han surgido a la hora de implantarlo y de cómo estas aumentan conforme el tamaño y los recursos de las entidades que deben aplicarlo disminuyen. Hay varios ejemplos de cómo las empresas de menor tamaño se

enfrentan a retos como: la falta de conocimiento (10), el alto coste de implantación e incertidumbre regulatoria (11).

1.1 Motivación

El desarrollo económico ha permitido durante años la mejora del nivel de vida de los ciudadanos de todo el planeta. Este desarrollo no sería posible sin el papel que juegan las microempresas, las pequeñas y medianas empresas (PYMES) y, en concreto, el pequeño comercio. La versatilidad y el dinamismo de estos negocios permite irrumpir en el escenario económico con ideas disruptivas; ideas que, en grandes empresas, probablemente serían aplastadas bajo el peso de los procesos ya asentados, los cuales muchas veces solidifican e impiden la introducción de grandes cambios a un coste asumible.

«Una cadena es tan fuerte como su eslabón más débil» esta frase atribuida al filósofo inglés Thomas Reid, es plenamente aplicable a la implantación del marco normativo del derecho a la protección de los datos personales. Las PYMES y las microempresas, son las que más problemas tienen a la hora de aplicarlo (12). Esta frase no debe entenderse en términos peyorativos, si no como una constatación de la escasez de recursos presente en las fases iniciales de crecimiento de un negocio. Una pequeña empresa tiende a concentrar sus escasos recursos en el desarrollo del negocio, dejando de lado otros aspectos importantes, pero no prioritarios. Sin embargo, sería un error afirmar que la protección de datos no es una parte fundamental del desarrollo del negocio; nadie desarrollaría su negocio ignorando el derecho a la vida, y nadie debería desarrollar su negocio ignorando el derecho a la protección de datos. Los esfuerzos para incrementar el porcentaje de implantación de la normativa en las PYMES han sido numerosos. En particular, las autoridades de control como, AEPD[1], CNIL[2] o ENISA[3], entre otras, han desarrollado múltiples guías y herramientas para facilitar la implantación de la normativa.

En el ámbito de las PYMES hay diversos sectores y subdivisiones, uno de ellos es el denominado pequeño comercio. Este grupo puede entenderse como pequeñas tiendas familiares, que generalmente carecen de estructura societaria y constan de un único establecimiento. Por ejemplo: fruterías, panaderías, farmacias, zapaterías, tintorerías, hostales, restaurantes, etc. Hoy en día, estos negocios afrontan una miríada de retos a los que deben enfrentarse para permanecer relevantes y competir en un mundo cada vez más digitalizado que pone una infinidad de opciones a nuestro alcance. Para que estos comercios puedan competir, tienen que desarrollar nuevas formas de presencia y relación con el cliente que se adapten al mundo digitalizado en el que vivimos. Por los motivos anteriores, se hace necesario ahondar en los esfuerzos para completar la implantación del marco normativo de protección de datos en el pequeño comercio. Si queremos seguir prosperando, el pequeño comercio no puede quedarse atrás.

1.2 Objetivos

El pequeño comercio es fundamental para el desarrollo económico y el cumplimiento del marco regulatorio y es esencial para que existan unas bases sólidas sobre las que sustentar dicho desarrollo. Pero ¿a qué nos referimos exactamente cuando hablamos de pequeño comercio? Podemos empezar acudiendo a la recomendación de la comisión europea sobre la definición de microempresas, pequeñas y medianas empresas (13). Para el asunto que nos ocupa, nos centraremos en las empresas de menor tamaño, las denominadas microempresas. Sin embargo, dentro de esta categoría podemos encontrar todo tipo de empresas, algunas de las cuales, cuentan ya con recursos propios suficientes para hacer frente a las necesidades surgidas de la implantación

[1] Agencia Española de Protección de Datos (AEPD) https://www.aepd.es
[2] Commission Nationale de l'Informatique et des Libertés (CNIL) https://www.cnil.fr/en
[3] European Union Agency for Cibersecurity (ENISA) https://www.enisa.europa.eu

del reglamento. Para acotar un poco más, introducimos la definición de la ley de ordenación del comercio minorista (14), que en su artículo 1.2 dice *«(...) se entiende por comercio minorista aquella actividad desarrollada profesionalmente con ánimo de lucro consistente en ofertar la venta de cualquier clase de artículos a los destinatarios finales de los mismos, utilizando o no un establecimiento»*.

Estas dos definiciones nos acercan desde la perspectiva legal al concepto de pequeño comercio. Sin embargo, es necesario aportar una definición consolidada que incluya algunos negocios del sector servicios no necesariamente incluidos desde la perspectiva legal. Así pues, introducimos la siguiente definición de pequeño comercio: todo negocio que pueda ser clasificado como microempresa, aunque no necesariamente posea una estructura societaria; que desarrollen profesionalmente con ánimo de lucro la venta de productos o servicios en un ámbito reducido; y que generalmente conste de un único establecimiento. Dentro de este grupo podemos encontrar pequeños negocios familiares como, fruterías, panaderías, farmacias, ópticas, etc., pero también negocios del sector servicios como, tintorerías, hostales, restaurantes, cines de barrio, dentistas, podólogos, etc.

Los objetivos que se pretenden alcanzar con el desarrollo de una guía para el cumplimiento de la normativa relativa a la protección de datos en el pequeño comercio son los siguientes:

- Construir un sistema de gestión centrado en el reglamento general de protección de datos adaptado al pequeño comercio
    - Aportar 4 ejemplos de implantación del sistema de gestión en distintos escenarios
    - Diseñar una metodología de prueba que permita validar y mejorar el sistema de gestión una vez implantado

1.3 Impacto

Este trabajo pretende ahondar en los esfuerzos hasta ahora llevados a cabo para implantar satisfactoriamente el marco normativo para garantizar el derecho a la protección de datos dentro de la Unión Europea. En concreto, pretende servir de muleta para que el pequeño comercio pueda, finalmente, completar el salto al mundo digital y mantener el estatus que ahora tiene dentro de nuestras sociedades evitando su desaparición.

1.4 Metodología

Es fundamental para la consecución de los objetivos establecer una serie de requisitos que deben cumplirse para que el resultado del trabajo pueda ser aplicado en el pequeño comercio. Aunque es posible que haya comercios que cumplan en cierta medida con algunos aspectos del reglamento, supondremos: que la implantación se realiza desde cero, que los conocimientos de la normativa son escasos, que el comercio no está familiarizado con los sistemas de gestión definidos en normas ISO, que los negocios en cuestión no disponen de ningún empleado especializado en informática y que no disponen de personal capacitado para la implantación correcta de medidas técnicas. Dadas estas limitaciones será muy importante que la solución busque minimizar la cantidad de recursos que la empresa debe disponer para su implementación.

Para alcanzar el cumplimiento de los requisitos establecidos en el reglamento es necesario conocer aspectos particulares de cada negocio que difícilmente son generalizables. Sin embargo, hay aspectos del grupo de negocios que son comunes, permitiendo establecer un procedimiento estándar que permita su extensión a casos particulares. Por tanto, se definirán unos casos de uso comunes sobre los que se aplicará la solución desarrollada.

Un aspecto relevante de los supuestos establecidos es la falta de conocimiento del marco normativo y de los procesos de auditoría y cumplimiento. Por tanto, todas las acciones de la

solución a desarrollar deben tener un fuerte componente formativo. De esta forma, no solo se implanta una solución, sino que se conciencia y forma al negocio para que la solución implantada se mantenga efectiva y actualizada a lo largo del tiempo.

Finalmente, habrá que diseñar puntos de extensión de la solución para que aquellos aspectos no cubiertos puedan ser desarrollados de forma autónoma, aspectos complejos como el análisis de riesgos o el análisis de impacto son necesarios para el cumplimiento en algunos ámbitos dentro del alcance. Sin embargo, no es posible desarrollar una solución general ya que los detalles son muy relevantes. Por este motivo, es necesario que la solución incluya los medios necesarios que permitan integrar estos elementos de diversas formas.

1.5 Estructura

Esta memoria pretende ser un informe del proceso de desarrollo completo de la solución propuesta. El primer apartado, la introducción anterior, ha situado en contexto el problema que se pretende abordar, cuál es la motivación para abordarlo, los objetivos que se pretenden alcanzar con el desarrollo propuesto y el impacto que se espera tenga en el ámbito de aplicación de la solución.

A continuación, se lleva a cabo una búsqueda bibliográfica con el objetivo de conocer con detalle el problema que se pretende solucionar, así como las soluciones ya existentes que intentan abordar el problema desde diferentes perspectivas. Se estudiarán estas soluciones en detalle, prestando especial atención a las similitudes y diferencias entre los ámbitos para los que se desarrollaron y el ámbito en el que queremos desarrollar nuestra solución. En esta sección se hace hincapié en las lagunas de dichas soluciones y en los motivos por los que no son de aplicación al problema al que nos enfrentamos. Finalmente, se hace una propuesta para rellenar las lagunas identificadas o problemas que los autores detectaron, pero decidieron no resolver en la solución que desarrollaron.

Conocido el estado de la cuestión y la propuesta para aportar una solución a los problemas detectados, se procede al análisis de los requisitos que dicha solución debe cumplir para mejorar las ya existentes. El análisis de requisitos abordará, punto por punto, los distintos enfoques que la solución a desarrollar puede tomar y cuáles de ellos son los más adecuados para alcanzar los objetivos propuestos. Un claro ejemplo de las variables que intervienen en el análisis de soluciones para un requisito dado, son el coste económico y el impacto que este puede tener en el desarrollo del negocio.

Llegados a este punto conocemos: los puntos de mejora que una solución que aborde el problema debe tratar, las distintas formas de abordar las mejoras y el impacto que cada una de estas propuestas puede tener sobre las empresas donde se desea implantar. Con toda esta información, podemos llevar a cabo un diseño completo de la solución. Este diseño buscará la mejor forma de materializar las soluciones escogidas en un documento, o serie de documentos, que sirvan de guía y que, en definitiva, constituyan el sistema de gestión que se pretende construir para cumplir los objetivos propuestos en este trabajo.

En el apartado 5, desarrollo de la solución, nos centramos en explicar aquellos aspectos más importantes del desarrollo y en cómo se tradujo el diseño a documentos reales. También se busca poner el foco en aquellas decisiones que, sin duda, son el punto diferenciador de esta propuesta, así como aportar el razonamiento que hay detrás.

El apartado de implementación se centra en proponer una metodología de implantación de la solución en el pequeño comercio. Este trabajo no aplica la solución desarrollada en un negocio real. Sin embargo, se decide implantar la solución sobre un negocio ficticio que represente el mayor número de casuísticas posibles. En concreto, este apartado intentará simular todo el proceso de implantación paso a paso. Se mostrará el orden que debe seguir el proceso y el tiempo esperado del proceso de principio a fin.

Aunque en este trabajo se busca mejorar las propuestas actuales, no pretendemos asumir que la solución desarrollada será completa y perfecta para todos los negocios. Es por esto por lo que, en el apartado de pruebas, se desarrolla una propuesta de validación del sistema implantado. Se plantearán preguntas como: ¿Se ha implantado correctamente la solución? ¿Se adapta el sistema a situaciones no previstas en el diseño inicial? ¿Es posible incorporar mejoras al sistema?

Finalmente, se concluirá este trabajo haciendo una revisión de lo conseguido. Se analizará el resultado final y se comparará con los objetivos iniciales, en particular, en que grado han sido estos alcanzados. También se analizará el resultado buscando posibles puntos de mejora o aspectos que, bien por falta de medios o por haber quedado fuera del alcance, no hayan sido incluidos en este trabajo. Estas propuestas de mejora podrían ser en el futuro el germen de un nuevo trabajo que permita mejorar la solución alcanzada.

2 Estado de la cuestión

Desde la entrada en vigor del reglamento general de protección de datos (8) se han identificado múltiples retos para su completa implantación. En concreto, en PYMES y microempresas se han identificado problemas como: la falta de conocimiento, la falta de personal cualificado o la incertidumbre regulatoria (10–12). Debido a la importancia de la implantación completa del reglamento para que la protección del derecho sea eficaz, se ha producido un esfuerzo colectivo para ayudar a conseguir que el cumplimiento sea total para todas las partes implicadas. Desde el mundo académico, han aparecido diferentes propuestas para crear un modelo que permita implantar el nuevo marco normativo dentro de una PYME (15, 16). Asimismo, se han desarrollado propuestas para la implantación en casos de uso concretos (17, 18). Y también se han desarrollado modelos para analizar el estado de cumplimiento (19). Por otro lado, también en el sector privado, han aparecido múltiples empresas que ofrecen servicios de consultoría para PYMES. Estas empresas tienen como objetivo de implantar el marco normativo dentro de otros negocios, por ejemplo, PYMELegal[4], Edorteam[5] o rgpdparapymes[6].

Por parte de los estados, los esfuerzos para mejorar el grado de implantación del nuevo reglamento han estado capitaneados por las propias autoridades de control, ya que el propio reglamento asigna entre sus funciones la concienciación y sensibilización de la población. Para ello, las diferentes autoridades de control han publicado manuales y guías con el objetivo de poner en conocimiento las acciones que deben ser llevadas a cabo por las empresas para cumplir con el marco normativo. ENISA publicó en 2016 una guía para el tratamiento de datos en PYMES (20), mientras que la AEPD ha publicado, entre otras, una guía para responsables del tratamiento (21) y herramientas, como FacilitaRGPD[7]. Estas guías y herramientas tienen el objetivo de ayudar a simplificar el proceso para alcanzar el cumplimiento en los casos más sencillos. Estos esfuerzos, son similares a los que han llevado las diferentes autoridades de control de los distintos países de la Unión Europea, por ejemplo, la autoridad de control francesa, CNIL, publicó la herramienta GDPR toolkit[8] para asistir en la implantación y desarrolló una guía práctica (22).

No obstante, no es posible crear una única solución que abarque todos los casos de uso. Los detalles de la implantación están supeditados al nivel de riesgo al que se expongan los datos personales durante su tratamiento. Es por ello, que cada vez más, los esfuerzos se centran en definir los casos de uso más comunes y, partiendo de ese alcance reducido, se crea un proceso de implantación enfocado a adaptar un área restringida a la normativa. El ámbito laboral es uno de los más comunes dada su ubicuidad (18), también en el ámbito de las bases de datos (17). Otros esfuerzos se centran en segmentar el universo de empresas por su tamaño y, especialmente, se centran en aquellas empresas que menos recursos tienen para afrontar la implantación del nuevo marco normativo (15). Aunque el marco normativo es diferente estos retos no son particulares del nuevo reglamento. En el marco español previo al nuevo reglamento, ya existían intentos de facilitar la implantación de la ley de protección de datos (4) en las PYMES (23).

2.1 Crítica a la situación actual

Toda la evidencia disponible apunta a que la implantación de la nueva normativa está siendo lenta, probablemente porque afecta a todos aquellos que traten datos personales sin ninguna excepción, excluyendo los casos en los que el propio reglamento permite acudir a normas específicas ya establecidas, como el secreto profesional. Además, elementos como el enfoque

[4] PYME Legal https://www.pymelegal.es
[5] Edorteam https://edorteam.com/consultoria-rgpd-empresas-pymes/
[6] RGPD para PYMEShttps://rgpdparapymes.net
[7] Facilita RGPD (AEPD). https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd
[8] GDPR toolkit (CNIL). https://www.cnil.fr/en/gdpr-toolkit

basado en riesgos hacen que su aplicación en las PYMES suponga una pronunciada curva de aprendizaje (24). La mayoría de las empresas de reducido tamaño carecen de sistemas de gestión y de procedimientos formales que permitan demostrar el cumplimiento. Es decir, no solo basta con implementar las medidas necesarias para garantizar la seguridad del tratamiento de los datos, sino que es necesario poder demostrar a la autoridad de control que se cumple con el marco normativo. Una implementación satisfactoria de medidas de protección sin la capacidad de auditar el cumplimiento no evitará la imposición de multas por incumplimiento.

En la literatura encontramos ejemplos de aplicación a casos de uso concretos como la guía para la implantación del RGPD en el entorno laboral (18), en la que se establecen algunos requisitos documentales necesarios para dar cumplimiento a la norma. Sin embargo, no establece medidas técnicas concretas ni procedimientos auditables, hay una gran falta de concreción que permita prever el éxito de la implantación en PYMES sin conocimientos previos. Por otro lado, la guía del cumplimiento para la protección de bases de datos (17), establece algunos procesos y aporta plantillas documentales para evidenciar el tratamiento, pero no establece procedimientos a seguir. En estos casos, el éxito quedará también condicionado a la experiencia previa en sistemas de gestión y en protección de datos. Finalmente, en adaptación de una PYME a la normativa RGPD (15), se establece la implantación dentro de un proceso PDCA (Plan, Do, Check, Act). Además, establece procedimientos formales, casos de uso concretos y medidas técnicas necesarias, aunque sin entrar en el detalle de su implementación. Sin embargo, el principal problema, es que asume en el ejemplo de implantación que la empresa dispone de un sistema de gestión de calidad ISO9001.

Por lo general, se suele establecer el requisito de conocimientos informáticos para aplicar las medidas, esto no siempre va a ser posible en el pequeño comercio. También se suele asumir cierta familiaridad con sistemas de gestión y auditorías algo a lo que, salvo en casos concretos, el pequeño comercio tampoco está acostumbrado. Estos son dos elementos clave que deben incluirse desde el comienzo en cualquier solución que pretenda diseñar una solución para implantar el marco normativo de protección de datos.

2.2 Propuesta

La propuesta que pretende desarrollar este trabajo se debe centrar en contribuir a facilitar la implantación del reglamento en pequeños comercios. En especial, debe de cubrir las lagunas identificadas en las soluciones ya existentes como: la ausencia de personal especializado en el ámbito de la informática, la ausencia de procesos formales establecidos y la ausencia de sistemas de gestión definidos en normas ISO. En línea con otras soluciones propuestas, nos centraremos en casos de uso comunes del pequeño comercio como puedan ser: la gestión de empleados, la gestión fiscal, la relación con el cliente, el marketing y el comercio electrónico. Con estos casos no se alcanza una cobertura al 100% de las actividades del pequeño comercio, pero se establece un punto de partida sobre el que extender la solución a nuevos casos de uso. Finalmente, es fundamental que la solución propuesta permita auditar el sistema implantado, de lo contrario no será posible garantizar el cumplimiento.

Para cumplir con lo expuesto en el párrafo anterior se propone desarrollar un sistema de gestión adaptado al pequeño comercio. Este sistema de gestión se puede entender como una suerte de norma ISO específicamente adaptada al pequeño comercio. Por tanto, este sistema definirá los procesos necesarios para la gestión de datos personales de acuerdo con los requisitos impuestos por el Reglamento General de Protección de datos. Este sistema no puede incluir de forma completa todos los casos de uso. Por tanto, se propone que la solución aborde aquellos puntos que forman parte del día a día del negocio. Sin embargo, tiene que dejar claros aquellos puntos que, aunque no se abordan, son obligatorios. Estos puntos de extensión permitirán añadir soluciones que se adapten a cada negocio, independientemente de que estas sean aportadas externamente (mediante la contratación de servicios de asesoría) o internamente (mediante personal interno

especializado). Finalmente, destacamos que se pretende que la solución sea utilizada por el personal del negocio, tanto empleados como por la propiedad.

3 Análisis del problema

Nuestra propuesta para resolver el problema es la creación de un sistema de gestión que permita implementar los requisitos del Reglamento General de Protección de datos, adaptándolo al pequeño comercio. No queremos reinventar la rueda, este tipo de sistemas se utilizan en multitud de ámbitos, permitiendo implantar diferentes regulaciones en todo tipo de empresas. El ejemplo paradigmático de este tipo de sistemas son los propuestos por las normas ISO. Se basan en políticas y procedimientos. Además, se centran en un aspecto fundamental para el proceso de auditoría, las evidencias. Todas las regulaciones incluyen la función de inspección, sería absurdo imponer requisitos pero no definir un procedimiento para comprobar su cumplimiento.

Este trabajo se centra en la perspectiva del responsable del tratamiento. En general, el pequeño comercio gestiona datos que han obtenido directamente del cliente mediante un consentimiento explícito. Esto no excluye aquellos casos en los que el pequeño comercio subcontrata servicios que puedan requerir de cesión de datos. Es decir, excluimos el caso en el que el pequeño comercio toma el papel de encargado de tratamiento. Sin embargo, aunque no se aborden los procesos desde dicha perspectiva, la información proporcionada para la creación de contratos de encargado de tratamiento, así como la guía del sistema de gestión, deberían de ser más que suficientes para extrapolar el sistema a otras perspectivas.

Desde el punto de vista del responsable del tratamiento, la norma establece los requisitos que los negocios deben cumplir. Nuestro sistema, para ser útil, debe contar: con procesos que definan como se tratan los datos, procesos para atender la casuística a la que se enfrenta el negocio en el ámbito del tratamiento de datos personales y procedimientos de recogidas de evidencias. Los siguientes puntos son los aspectos más relevantes que nuestro sistema debe definir:

- Formación: Este aspecto es, sin duda, el más relevante. Implantar un sistema de gestión requiere de la colaboración de todo el personal implicado. Por tanto, será requerimiento que el sistema incluya procedimientos de formación en el tratamiento de datos personales.

- Protección de datos desde el diseño: siempre que el negocio trate datos personales, deberá diseñar un proceso de tratamiento. Indicará que datos se recogen y como se tratan. Lo más importante, este diseño aplicará los principios definidos en la normativa.

- Análisis de riesgos y de impacto: el proceso de diseño incluirá un análisis de riesgo básico sobre el tratamiento de los datos personales implicados. Además, existirán casos en los que un análisis de riesgos formal y un análisis de impacto no son solo recomendaciones si no requisitos exigidos por la norma. Por ejemplo, la gestión de datos salud (ópticas, farmacias…).

- Medidas técnicas de seguridad: Como resultado del análisis de riesgos realizado, se implementarán una serie de medidas técnicas de seguridad con el objetivo de mitigar los riesgos descubiertos para los datos personales tratados. No es un secreto que hoy en día la mayoría de las actividades de tratamiento involucran, de una manera u otra, las tecnologías de la información. Por tanto, es necesario implantar medidas técnicas de seguridad que garanticen la seguridad de los datos en dichos sistemas.

- Condiciones para la recogida y tratamiento de datos personales: Uno de los puntos fundamentales de la norma es identificar una base legitimadora para todas

y cada una de las actividades de tratamiento realizadas, así como la con la que finalidad se recogen.

- Obtención del consentimiento: aquellas actividades que estén legitimadas por el consentimiento explícito del interesado requerirán de una gestión del ciclo de vida del consentimiento.

- Registro de actividad de tratamiento: toda la información anterior será documentada en un registro que permitirá conocer en todo momento que actividades de tratamiento se realizan, como se realizan, donde se almacenan los datos y como se obtuvieron.

- Ejercicio de derechos: los propietarios de los datos personales tratados tienen una serie de derechos que deben ser satisfechos en tiempo y forma. Es necesario que exista un proceso de gestión auditable y que describa cómo el responsable del tratamiento atiende las solicitudes de ejercicio de derechos de los interesados.

- Contratos de encargado: dentro de un negocio habrá actividades de tratamiento que, por su naturaleza, sean gestionadas por un servicio externo. Este tipo de actividades, además de ser incluidas en el registro de actividades de tratamiento, requerirán de la firma de un contrato que asegure que los requisitos impuestos dentro del negocio para la protección de datos de carácter personal se cumplen, extendiéndolos a los procesos de tratamiento realizados por el encargado. De esta forma se garantiza que se mantienen los mismos estándares para los datos, independientemente de que la actividad se realice dentro o fuera del negocio.

- Transferencias internacionales y cesiones de datos: podría parecer extraño que un pequeño negocio vaya a entrar en este tipo de actividades. Sin embargo, la realidad es que hoy en día es una práctica habitual contratar software como servicio hospedado en la nube y, aunque hay centros de datos en prácticamente todos los países europeos, no existe la garantía de que todo el tratamiento se realice en un centro de datos nacional. Además, también pueden existir casos de cesión de datos en pequeños negocios, como el intercambio de datos entre empresas de un mismo grupo empresarial.

- Delegado de protección de datos: en la mayoría de los casos, un pequeño comercio no necesitará de un delegado de protección de datos. Sin embargo, es necesario que quede claro cuando es necesario contar con dicho representante.

Al margen de los requisitos propios de la norma, tenemos que considerar aquellas lagunas o puntos de mejora descubiertos durante la revisión de la literatura existente. Una de las lagunas más importantes, es la referida a los procesos de inspección y auditoría. La mayoría de los recursos disponibles, se centran en la formación y la implantación. Sin embargo, obvian los procedimientos que deben seguirse para poder demostrar el cumplimiento. Por otro lado, los procesos de implantación descritos carecen de ejemplos de aplicación. Sin ejemplos y metodologías adaptadas es muy difícil, para personas sin conocimientos previos, implantar un sistema de gestión satisfactoriamente. Es por ello por lo que uno de los requisitos será aplicar nuestra metodología de implantación sobre ejemplos concretos (ficticios). Estos ejemplos permitirán comprender como será el día a día de un negocio durante y después de la implantación del sistema. Finalmente, sería arrogante suponer que el sistema que desarrollemos será perfecto. Por tanto, será necesario definir un procedimiento de prueba. Este procedimiento deberá ser capaz de verificar el estado de implantación del sistema y de proponer mejoras para aquellas deficiencias que se detecten.

3.1 Identificación y análisis de soluciones propuestas

Como ya se ha comentado anteriormente, los sistemas de gestión son utilizados en muchos ámbitos distintos. Aunque siempre comparten el objetivo de definir procesos reproducibles y verificables para garantizar el cumplimiento de una serie de requisitos. Es por ello que existen multitud de soluciones disponibles para la incorporación de estos sistemas en un negocio:

- **Asesorías o gestorías:** Prácticamente todo negocio, independientemente de su naturaleza jurídica, cuenta con servicios externos que gestionan ciertos ámbitos burocráticos del negocio. Estos servicios se han centrado tradicionalmente en la gestión de los aspectos fiscales, jurídicos y laborales, aspectos que son comunes a todos los negocios. Estos negocios son la personificación (natural o jurídica) del principio de división del trabajo y las economías de escala. Su personal está especializado y altamente formado en los temas que abordan. Además, gestionan al mismo tiempo múltiples negocios, lo que proporciona experiencia para diseñar procesos comunes y eficientes. Pese a lo anterior, es común que la aplicación del RGPD quede restringida a los ámbitos ya gestionados. Por ejemplo, los contratos laborales gestionados por estos servicios cumplirán con la normativa laboral y de protección de datos de carácter personal. Sin embargo, estos servicios no alcanzan las necesidades reales para el cumplimiento completo de la norma, dejando de lado aspectos relevantes que no están incluidos en el servicio contratado. Como ejemplo de esto, podemos encontrar noticias que relatan como un empleado despedido por sustraer mercancía es readmitido en la empresa. Esta readmisión se debió a que su contrato laboral no incluía información relativa al sistema de videovigilancia, suponiendo una violación de los derechos fundamentales del empleado. Este tipo de casos son una muestra de los retos a los que se enfrentan las empresas. Desconocemos los hechos particulares que llevaron a esta situación, pero podemos especular y concluir lo siguiente. Por un lado, la gestoría no hizo lo suficiente para conocer la realidad del negocio, obviando el hecho de que existía un sistema de videovigilancia de los empleados; por otro lado, el desconocimiento por parte de la empresa de las implicaciones de contar con un sistema de videovigilancia llevó a no notificar a la gestoría de forma proactiva. Este es un claro ejemplo en el que la falta de una solución personalizada y el desconocimiento de la norma pueden causar un perjuicio económico y laboral. Finalmente, hay que destacar que estos servicios, no necesariamente incluyen otros aspectos relevantes que quedan fuera de su ámbito de trabajo tradicional. Imaginemos que el negocio quiere proporcionar un boletín informativo a sus clientes. En estos casos, es necesaria la recogida del consentimiento y todo lo que ello implica. Por defecto, esto será un servicio no incluido y que habrá que contratar por separado. Además, hay que tener en cuenta que la empresa de asesoría no necesariamente ofrecerá este tipo de servicios.

- **Consultora especializada**: Al igual que existen gestorías para los ámbitos fiscales, jurídicos y laborales. Hay empresas de consultoría que se especializan en RGPD e implantación de todo tipo de normas (como normas ISO) o regulaciones, ofreciendo un servicio completo y personalizado. Estas empresas, al igual que las gestorías, son un ejemplo más de la división del trabajo y las economías de escala, ya que cuentan con personal especializado capaz de proveer el servicio a múltiples empresas al mismo tiempo. Otra ventaja que ofrecen estas empresas es que, con el tiempo, han desarrollado procesos que pueden aplicar a varios casos distintos, facilitando la implantación y reduciendo el tiempo necesario para alcanzar el cumplimiento. Sin embargo, es una realidad que dentro del universo de empresas que contratan estos servicios, hay un gran número de

variaciones, por lo que siempre habrá casos en los que no existan procesos previos, teniendo que definirse para un caso concreto. Es por lo anterior, que este tipo de servicios son personalizados y adaptables a cada caso concreto y, en definitiva, suponen un coste elevado. Además, en los últimos años, el número de requisitos regulatorios ha aumentado significativamente. Podemos encontrar como se han aprobado nuevas regulaciones como DORA o revisiones aprobado revisiones de otras ya existentes que han expandido su ámbito de aplicación (ENS, NIS 2…). Lo anterior, ha provocado que estas empresas estén experimentando una falta de personal que provoca: una alta carga de trabajo; aumento de la rotación laboral, causando perdida de conocimiento y, en definitiva, un peor servicio. Lo que a priori parece el punto fuerte de este tipo de negocios (el servicio personalizado), se ha convertido en su talón de Aquiles, el proceso inicial de toma de requerimientos no es escalable. Este hecho, junto a la falta de personal, deriva en dos posibles consecuencias. La ausencia de suficiente oferta de estos servicios como para cubrir la demanda o la simplificación del proceso. Esta última supone correr el riesgo de no descubrir todos los aspectos relevantes del negocio afectados por la regulación.

- **Implantación autogestionada:** Como con cualquier parte del negocio, siempre existe la posibilidad de construir una solución personalizada desde dentro. Para hacerlo se puede contratar personal especializado o que sea el propio empresario el que capitanee los esfuerzos, bien por contar con experiencia previa, bien centrándose en los aspectos nucleares, subcontratando aspectos más específicos.

  Llevar a cabo un proceso de contratación de personal especializado es una tarea ardua. En la mayoría de los casos, el entrevistador carecerá de los conocimientos necesarios para determinar si un potencial empleado cumple con los requisitos para llevar a cabo la tarea de implantación y mantenimiento de la normativa. Pero, aunque se pudiera evitar este problema, el negocio se seguirá enfrentando al elevado coste que supone crear un puesto de este tipo cuando no es la actividad principal del negocio. Esta opción se ha incluido por completitud, pero se entiende que en la mayoría de los casos quedará completamente descartada. El tipo de negocios que estamos analizando, son parcos en recursos económicos y se limitan al personal esencial. Por tanto, tienden a externalizar todos aquellos aspectos del negocio que sean susceptibles de serlo.

  Otra de las opciones mencionadas es el modelo autogestionado. Habrá casos (probablemente pocos), en los que el empresario contará con los conocimientos técnicos y jurídicos necesarios para llevar a cabo la tarea con éxito. Imaginemos que un exempleado de un departamento de informática, plenamente involucrado en la implantación y mantenimiento de sistemas de gestión del Reglamento General de Protección de Datos y normas ISO (como la ISO27001), decide montar su propia empresa. Seguramente, será capaz de realizar la mayoría de las tareas, pudiendo contar con apoyos puntuales. Sin embargo, el caso central, será el de un empresario capaz de realizar todas las tareas necesarias, simplemente tomando como referencia los recursos publicados por: autoridades de control, universidades, blogs de consultoras y auditoras… En general, este modelo será el más económico, por lo menos en términos monetarios. No obstante, este modelo entraña riesgos. Hay aspectos de la norma que son ambiguos y, sin experiencia previa, difíciles de implementar correctamente. Aunque siempre se puede contar con apoyo externo de manera discrecional en aquellos aspectos que sean fuente de ambigüedad.

Implantar y mantener un sistema de gestión suele ser un proceso elaborado. Dada la complejidad que puede llegar a alcanzar en sistemas grandes existen softwares para llevar a cabo esta tarea. Estos softwares suelen ser caros y requieren de conocimientos previos y muy específicos. Dentro del ámbito de la protección de datos, pueden existir versiones más reducidas y económicas. Sin embargo, suelen estar muy ligados a la gestión de la seguridad de la información y el coste final puede seguir siendo inasumible para un pequeño comercio. Una alternativa a estos sistemas es desarrollar el sistema de gestión como una estructura organizada de documentos y evidencias, utilizando el sistema de archivos de cualquier dispositivo informático. Para grandes sistemas sería inmanejable, ya que daría lugar a estructuras en las que sería muy difícil encontrar la información. Sin embargo, en sistemas pequeños es versátil, fácil de comprender sin conocimientos previos (cualquiera que use un ordenador entiende un sistema de archivos) y sencillo de gestionar. Finalmente, si el negocio crece este sistema siempre se puede migrar a una solución más compleja.

Hay una serie de aspectos que son los más conocidos por el público general, cualquiera que haya leído un formulario de recogida de datos se ha enfrentado a algunos de los siguientes conceptos:

- Diseño de actividades de tratamiento
  - Principios de tratamiento
  - Bases legitimadoras
  - Obtención del consentimiento
- Cesión de datos a terceros
  - Cesión intragrupo, cambios de responsable
  - Transferencias internacionales
  - Encargados de tratamiento

Existen multitud de recursos que explican, proporcionan plantillas y ejemplos de los casos anteriores. Estos recursos, principalmente creados por las autoridades de control, están disponibles para cualquiera con acceso a internet. Sin embargo, estos recursos se proveen con mayor o menor detalle, son modelos tipo que no necesariamente son aplicables a todos los casos y, en general, no hacen ninguna mención a la recogida de evidencias. También se pueden utilizar de forma discrecional servicios de asesoría y consultoría externos que asistan en el desarrollo e implementación de forma puntual, con el consiguiente coste económico.

En cuanto al resto de requisitos, existen distintos tipos de soluciones y requieren de una revisión un poco más elaborada:

- **Formación:** la formación básica es fundamental para cualquier implicado en el tratamiento de datos. Para el caso que nos ocupa, suponemos que el negocio emplea al empresario, dueño del negocio, y al menos a un empleado. Ambos deben de disponer de los conocimientos básicos para: llevar a cabo los procesos definidos del sistema de gestión, conocer el vocabulario relacionado con la protección de datos, atender las solicitudes realizadas por los interesados y colaborar en la definición de las actividades de tratamiento. Esta formación puede obtenerse de maneras diversas, pero nos centramos en dos en concreto:

  - **Cursos de formación:** siempre es posible encontrar ofertas de cursos de formación específicos en protección de datos. Estos cursos pueden ser de centros de formación permanente[9], proporcionados por las propias consultoras, etc. Es posible que incluso puedan ser financiados por mecanismos como Fundae[10] (en

[9] Curso RGPD (UPV). https://www.cfp.upv.es/formacion-permanente/curso/reglamento-general-proteccion-datos-dia-dia-responsables-encargados-tratamiento-datos_74373.html

[10] Fundae. https://www.fundae.es

España). Como es de esperar, estos recursos suponen un desembolso económico que, aunque no suele ser excesivo, puede no ser adecuado para todos los negocios.

- **Formación abierta:** existen multitud de recursos online que permiten la formación autodidacta en los aspectos básicos de la normativa de protección de datos. Hay recursos creados por las autoridades de control, en video[11] o por escrito(21, 22). También existen recursos de formación abierta proporcionados por Universidades como la UPV[12,13]. Estos recursos son gratuitos, sin embargo, no necesariamente siguen una estructura didáctica y, generalmente, carecen de un tutor que pueda guiar el aprendizaje y resolver dudas.

- **Análisis de riesgos y análisis de impacto:** existen diversas metodologías para llevar a cabo estos análisis, así como guías y los propios requisitos definidos por la norma. Sin embargo, estos análisis suelen implicar varios parámetros y requieren de un conocimiento amplio de diversos factores de riesgo relacionados con ciertos datos. Como en muchos casos podemos subdividir las posibles soluciones en dos grupos:

  - **Autogestionado:** existen recursos formativos abiertos y formación específica para llevar a cabo estos procesos. La formación puede implicar un coste económico. El responsable último del análisis de riesgos es el responsable del tratamiento y, en definitiva, el encargado de realizarlo y documentarlo. Esta solución se enfrentará a las diversas metodologías de análisis de riesgos disponibles y a una gran ambigüedad inherente a la definición de estos procesos. Esto último, puede acarrear un gran esfuerzo y expone al negocio al riesgo de un resultado incorrecto en ausencia de experiencia previa.

  - **Subcontratar:** esta opción se basa en acudir a empresas o individuos que sean capaces de proporcionar una ayuda específica para la definición y documentación de un proceso de análisis de riesgos. Esta solución implicará siempre un coste económico.

- **Medidas técnicas de seguridad:** uno de los aspectos fundamentales de la norma es la seguridad de los datos tratados, independientemente de que su tratamiento se realice mediante elementos electrónicos o no. La idea principal de este trabajo es que el tratamiento siempre se realizará mediante soportes electrónicos pero esta suposición no es un requisito. Nada impide que se gestione el sistema a la antigua usanza (papel y archivadores). En esos casos, las medidas técnicas de seguridad pueden quedar reducidas a sistemas de videovigilancia y compartimentos cerrados donde almacenar la información de forma segura. Sin embargo, si abrimos la puerta a opciones más modernas, el conjunto de medidas de seguridad técnicas se expande y puede entrar en terrenos que requieran de conocimiento específico. Las soluciones a estos casos se pueden agrupar en dos conjuntos:

  - **Autogestionadas:** esta opción requiere de conocimientos específicos en el ámbito de la informática que, en algunos casos, puede no estar al alcance de todo el mundo. Las autoridades de control han generado guías que detallan las medidas

[11] Formación protección de datos (AEPD). https://www.youtube.com/playlist?list=PLmwuU-8TVYMwbubYfXoRR50g2qaLmQ6dT

[12] Protección de datos (UPV). https://www.youtube.com/watch?v=WW1IJfcQ2xs

[13] RGPD (UPV) https://www.youtube.com/watch?v=y1hO3P5hFTw

de seguridad que deberían implementarse y cómo hacerlo en algunos casos. Estos recursos pueden ser más que suficientes para implementar un gran porcentaje de las medidas de seguridad. Además, últimamente ha habido una explosión de asistentes de inteligencia artificial generativa que son perfectamente capaces de explicar cómo implementar una medida técnica de seguridad. Estos recursos son gratuitos, pero al igual que con la formación pueden requerir de un esfuerzo extra.

- Subcontratadas: como con cualquier otro servicio, siempre es posible encontrar empresas o individuos que ofrezcan soporte discrecional para la gestión de sistemas informáticos. En estos casos, siempre será el responsable del tratamiento el que defina las medidas de seguridad que deben ser implementadas, pudiendo subcontratar su implementación. Por supuesto, estos servicios tienen un coste económico.

- **Ejercicio de derechos**: uno de los requisitos más importantes del reglamento general de protección de datos, y que más quebraderos de cabeza puede suponer, es el ejercicio de derechos de los interesados. Este punto puede llegar a ser complejo de gestionar, además el ejercicio de derechos es discrecional y se imponen plazos cuyo incumplimiento lleva asociado sanciones y/o inspecciones de la autoridad de control.

  - Recientemente, han aparecido soluciones informáticas que facilitan la gestión de estos procesos. Estas soluciones se basan en software que almacena todo lo necesario para atender una solicitud de ejercicio de derechos. Sin embargo, es imposible automatizar completamente esta gestión ya que estos softwares no siempre van a disponer de acceso directo a los datos.

  - Un proceso personalizado se puede adaptar a cualquier situación. Requiere del diseño de procedimientos para tratar las solicitudes, como procesarlas y como resolverlas.

- **Delegado de protección de datos:** un delegado de protección de datos es una persona o entidad que se encarga de representar al negocio ante la autoridad de control y los interesados. No cualquiera puede ser delegado de protección de datos, dado que va a ser el representante en materia de protección de datos, debe contar con los conocimientos técnicos y jurídicos necesarios para llevar a cabo esta tarea. Sin embargo, la norma no exige una titulación específica. Pero si es importante que se acrediten conocimientos técnicos y jurídicos en la materia. Dada la especificidad y la exigencia de requisitos para este rol, podemos concluir que hay dos opciones disponibles:

  - **Contratar personal específico:** esta opción implicará la búsqueda y contratación de personal específico que se incorporará a la plantilla del negocio. Además, requerirá de un proceso de verificación de las acreditaciones necesarias y un proceso de contratación específico. Una vez contratado, deberán de llevarse a cabo los procesos de registro ante la autoridad de control. Por supuesto, esta opción conlleva un coste económico elevado en forma de salario.

  - **Contratar un servicio externo de delegado de protección de datos:** existen multitud de servicios que ofrecen a su personal como delegado de protección de datos para otros negocios. Este personal tomará el rol de delegado de protección de datos de nuestro negocio (y de otros muchos otros). Estas opciones tienen un

coste económico inferior y externalizan aspectos como el proceso especifico de contratación que pueden llegar a ser complejos.

3.2 Solución propuesta

Tras valorar todas las opciones disponibles, pasamos a elegir las soluciones que, en nuestra opinión, son más adecuadas para satisfacer los requisitos detectados y alcanzar los objetivos propuestos. La solución propuesta se aplicará sobre el pequeño comercio, por tanto, debemos tener en cuenta que: los recursos económicos son reducidos, el conocimiento previo en materia de protección de datos es escaso y existen multitud de retos adicionales a los que este tipo de negocios deben enfrentarse. Es por ello que la solución propuesta deberá centrarse en los aspectos fundamentales a incorporar en el día a día del negocio, externalizando los procesos no esenciales para el negocio y buscando apoyo externo para la implementación de los aspectos para los que no se posee el "*know-how*".

Por todo lo anterior, se ha decidido que el sistema de gestión se implemente mediante un sistema de carpetas organizado que sirva como base de conocimiento que defina procesos y archive evidencias. Este sistema será autogestionado, es decir, será el negocio el que se encargue de implantar el sistema y mantenerlo, llevando a cabo todas las tareas esenciales para garantizar el cumplimiento de la normativa en vigor de protección de datos personales. No obstante, ya se ha establecido que estos negocios se enfrentan a la escasez de recursos para llevar a cabo todas las tareas necesarias. Por tanto, el sistema propuesto tendrá un fuerte componente de externalización que buscará señalar aquellos aspectos que pueden ser externalizados y pondrá énfasis en recomendar la externalización de aspectos concretos.

En el apartado anterior, describimos con detalle los elementos más importantes y analizamos las posibles soluciones. En general, nuestra solución aplicará principalmente el modelo autogestionado sobre aquellos aspectos relativos al diseño y definición de actividades de tratamiento. Esta solución es la más indicada para el caso que nos ocupa, ya que el negocio conoce en detalle los datos que maneja y como los utiliza. Aunque la externalización de estos aspectos es posible, implica transmitir dicha información en una toma de requisitos. Creemos que este aspecto es el más difícil de realizar satisfactoria dada la reducida cantidad de recursos disponible para el pequeño comercio. Podemos decir lo mismo del problema general de la cesión de datos a terceros, pero con un pequeño matiz. Aunque será el negocio el de conocerá los datos, se puede contar con un servicio externo para la redacción de contratos de encargado del tratamiento.

La formación es, sin duda alguna, el aspecto más relevante. Es necesario que todos los implicados en el tratamiento de datos tengan un conocimiento básico. Para alcanzar este conocimiento escogemos utilizar los recursos abiertos. Como ya se ha comentado anteriormente, existe un amplio abanico de recursos formativos creados por profesionales del ámbito educativo y regulatorio, por lo que ahondar en este ámbito sería un intento de reinventar la rueda. No obstante, se dejará a la elección del negocio la posibilidad de contratar una sesión formativa o un curso completo si así lo desean. Aunque nuestra solución no desarrollará recursos formativos, si hará el esfuerzo de definir unos requisitos mínimos que cualquier acción formativa deberá cumplir. Finalmente, se hará hincapié en la toma de evidencias. Sea cual sea el método formativo escogido se requerirán certificados o declaraciones responsables firmadas por todo el personal que esté implicado en el tratamiento de datos personales y, por tanto, debe estar formado.

Otro aspecto relevante comentado en el análisis anterior es el referido al análisis de riesgos y la evaluación de impacto. El análisis de riesgos es obligatorio, sin embargo, en casos sencillos se puede realizar un análisis ad-hoc adaptado a cada situación. Nuestra solución propondrá un proceso de análisis de riesgos básico para estos casos. No obstante, dejará claro cuando se puede aplicar este proceso y cuando no. Si resulta que el caso abordado no puede utilizar el método

simplificado, no queda más remedio que recurrir a un servicio externo. Se buscará un apoyo puntual que permitirá, aportando que datos personales se utilizan y en que procesos, la aplicación de una metodología formal y la generación de evidencias conforme a la norma de todo el proceso de análisis de riesgos y evaluación de impacto (cuando proceda).

El proceso anterior de análisis de riesgos definirá su utilizará para establecer las medidas técnicas de seguridad que deben ser implementadas. Estas medidas servirán para mitigar los riesgos sobre las actividades de tratamiento de datos llevadas a cabo. Existen multitud de recursos disponibles, la inteligencia artificial generativa entre ellos para implantar medidas de seguridad técnicas más comunes. Nuestra solución incluirá aquellos procedimientos de implantación y recogida de evidencias para aquellas medidas que son independientes de cualquier aspecto externo. Por ejemplo, la fortaleza de las contraseñas. Sin embargo, habrá medidas que dependen completamente de aspectos que es imposible prever. Por tanto, se recomendará acudir a personal especializado para su implementación. Aunque las medidas sean implantadas por personal externo, se definirá un procedimiento a seguir. Este procedimiento hará énfasis en la necesidad de que, además de implantarse las medidas, se recojan evidencias de este proceso. Por último, nuestra solución incluirá una enumeración (no exhaustiva) de posibles medidas de seguridad.

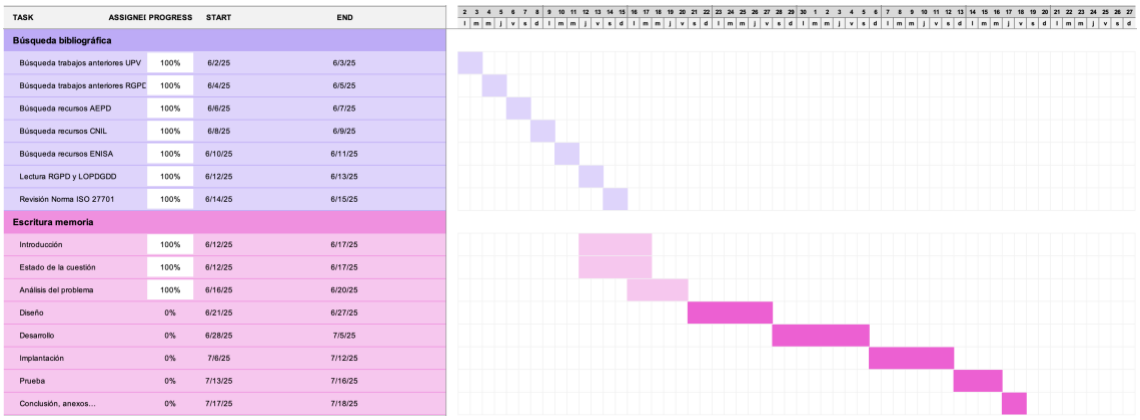
Uno de los puntos más complejos de implementar (complejo, pero no difícil) es el proceso para el garantizar que los interesados pueden ejercer sus derechos en materia de protección de datos personales. Nuestra solución desarrollará procesos, uno por cada derecho, que definirán como tratar y evidenciar la gestión de las solicitudes que pueda recibir el negocio.

El último de los requisitos asociados a la norma discutido en el apartado anterior fue el delegado de protección de datos. Nuestra solución exhortará a contratar un servicio externo de delegado de protección de datos. No consideramos que incorporar este perfil a la plantilla sea una solución adecuada. No obstante, se definirá un procedimiento que deje claro bajo que situaciones es requerida la contratación de este servicio y cuáles son los requisitos mínimos necesarios que un servicio de estas características debe cumplir. Especialmente, se requerirá que el servicio proporcione evidencias de que cumple con los requisitos.

Todo lo anterior servirá para construir el sistema de gestión propuesto para solucionar el problema al que nos enfrentamos. Sin embargo, todo el esfuerzo realizado sería en vano si nuestra solución no incorpora una guía de implantación y un procedimiento de prueba. El procedimiento de implantación definirá una metodología que, punto a punto, describirá los pasos a tomar para llegar desde la situación previa a un sistema completamente implantado. Para ello, se definirán una serie de escenarios ficticios sobre los que se aplicará el sistema, dando lugar a ejemplos prácticos que puedan guiar al usuario del sistema sobre su uso. En cuanto al procedimiento de prueba, se basará en dos aspectos fundamentales: los planes de acción correctiva y las declaraciones de aplicabilidad. Ambos procesos nos permitirán definir un proceso iterativo para reaccionar al descubrimiento de deficiencias del sistema de gestión y definir un procedimiento de revisión del estado global de cumplimiento.

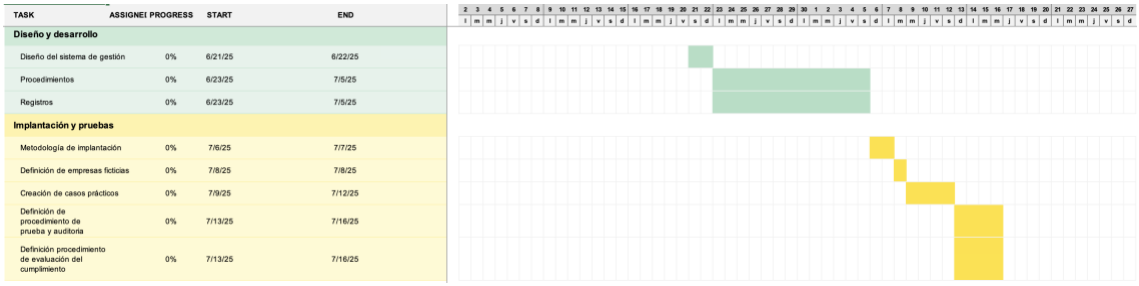
3.3 Plan de trabajo

Llegados a este punto es conveniente revisar el trabajo que llevamos hecho hasta el momento y aquello que queda por hacer. Para ello, se ha desarrollado un diagrama de Gantt con las tareas realizadas hasta la fecha y una previsión de aquellas pendientes de realizar, abarcando tanto la escritura de esta memoria como el propio desarrollo de la solución propuesta.



TASK	ASSIGNEE	PROGRESS	START	END
Búsqueda bibliográfica				
Búsqueda trabajos anteriores UPV		100%	6/2/25	6/3/25
Búsqueda trabajos anteriores RGPD		100%	6/4/25	6/5/25
Búsqueda recursos AEPD		100%	6/6/25	6/7/25
Búsqueda recursos CNIL		100%	6/8/25	6/9/25
Búsqueda recursos ENISA		100%	6/10/25	6/11/25
Lectura RGPD y LOPDGDD		100%	6/12/25	6/13/25
Revisión Norma ISO 27701		100%	6/14/25	6/15/25
Escritura memoria				
Introducción		100%	6/12/25	6/17/25
Estado de la cuestión		100%	6/12/25	6/17/25
Análisis del problema		100%	6/16/25	6/20/25
Diseño		0%	6/21/25	6/27/25
Desarrollo		0%	6/28/25	7/5/25
Implantación		0%	7/6/25	7/12/25
Prueba		0%	7/13/25	7/16/25
Conclusión, anexos...		0%	7/17/25	7/18/25

Figura 1. Diagrama de Gantt detallando las fases previas al desarrollo del trabajo, así como la escritura de la memoria.[14]



TASK	ASSIGNEE	PROGRESS	START	END
Diseño y desarrollo				
Diseño del sistema de gestión		0%	6/21/25	6/22/25
Procedimientos		0%	6/23/25	7/5/25
Registros		0%	6/23/25	7/5/25
Implantación y pruebas				
Metodología de implantación		0%	7/6/25	7/7/25
Definición de empresas ficticias		0%	7/8/25	7/8/25
Creación de casos prácticos		0%	7/9/25	7/12/25
Definición de procedimiento de prueba y auditoría		0%	7/13/25	7/16/25
Definición procedimiento de evaluación del cumplimiento		0%	7/13/25	7/16/25

Figura 2. Diagrama de Gantt detallando las fases de desarrollo del proyecto.[14]

Suponiendo una jornada de trabajo de 8 horas la duración total estimada del proyecto es de 376 horas. Sin embargo, hay que destacar que las estimaciones incluyen un margen de seguridad de una semana para contemplar posibles imprevistos que puedan surgir. Si no tenemos en cuenta este margen de seguridad se espera que el proyecto ocupe un total 320 horas de trabajo efectivo.

[14] Plantilla Simple Gantt chart. https://create.microsoft.com/en-us/template/simple-gantt-chart-4bf6b793-490f-4623-84ca-c9c6251a91fc

4 Diseño de la solución

El punto de entrada al sistema de gestión será una carpeta en el sistema de archivos del ordenador denominada SGSI RGPD, siglas de Sistema de Gestión de la Seguridad de la Información para el Reglamento General de Protección de Datos. Los sistemas de gestión definen procedimientos que describen como el negocio implementa los requisitos de la norma. Estos procedimientos deben ser verificables, por lo que se recogen evidencias como elemento de prueba. Nuestro sistema de gestión contará con dos elementos principales, la carpeta "Procedimientos" que contendrá todos los procedimientos y los asociará a un área temática. Por otro lado, la carpeta "Registros" contendrá todas las evidencias. Esta carpeta también estará segmentada por áreas temáticas, de forma que se pueda establecer una relación 1:1 con los procedimientos. Estas áreas temáticas toman como referencia la subdivisión en controles que propone la norma ISO 27701(25). No obstante, aunque pueda haber parecidos, la estructura seguida en este trabajo no será la misma. Esto es debido a que esa norma es una extensión de la norma ISO 27001(26) y, por tanto, habrá multitud de aspectos que excluimos intencionadamente para simplificar nuestro sistema de gestión al máximo.

4.1 Arquitectura del sistema

La arquitectura global del sistema de gestión es sencilla. Se ha buscado una organización que reproduzca el orden del proceso de implantación. De esta manera se aprenderá la estructura de forma implícita durante dicho proceso.

Procedimientos:

1. Formación
2. Actividades de tratamiento
    a. Actividad 1
3. Análisis de riesgos e impacto
4. Medidas técnicas de seguridad
5. Consentimientos
    a. Actividad 1
6. Ejercicio de derechos
7. Encargados de tratamiento
8. Delegado de protección de datos (DPD)

Registros:

1. Formación
    a. Empleado 1
2. Actividades de tratamiento
    a. Actividad 1
3. Análisis de riesgos e impacto
4. Medidas técnicas de seguridad
    a. Medida 1
5. Consentimientos
    a. Actividad 1
        i. Interesado 1
6. Ejercicio de derechos
    a. Interesado 1
        i. Acceso
        ii. Rectificación
        iii. Supresión
        iv. Limitación
        v. Portabilidad
        vi. Oposición
7. Encargados de tratamiento
    a. Encargado 1
8. Delegado de protección de datos (DPD)

Los sistemas de gestión evolucionan con el tiempo, es importante que dicho cambio quede registrado en el sistema. Para ello, los procedimientos irán acompañados de una carpeta "versiones antiguas" donde se almacenarán los procedimientos en el estado anterior a su última modificación.

4.2 Diseño detallado

Como ya se ha comentado en la sección anterior, nuestro diseño consta de dos elementos principales: procedimientos y registros. Los procedimientos son una serie de documentos escritos que describen los procesos que el negocio lleva a cabo para garantizar el cumplimiento. Estos procedimientos también establecen reglas que deben cumplirse dentro de la organización para garantizar el cumplimiento. Finalmente, definen que registros los acompañan como evidencia. Por otro lado, existen los registros. Estos registros, generalmente definidos en los procedimientos, son evidencias de que los procesos llevados a cabo por la organización se adhieren a lo definido en los procedimientos. Estas dos herramientas son necesarias y suficientes para garantizar el cumplimiento y poder demostrarlo ante la autoridad de control.

Empecemos analizando el diseño propuesto para los procedimientos. El primer elemento que se incluye es una plantilla Word con un formato predefinido. La inclusión de esta plantilla busca dos objetivos: garantizar la uniformidad en la estructura de todos los procedimientos y garantizar que todos los procedimientos incluyen una sección de versionado. Este último punto es necesario para asegurar que se registran los cambios realizados en los procedimientos, quien los realiza y quien los aprueba. Analicemos ahora el diseño propuesto para cada procedimiento:

- Formación: el procedimiento de formación diseñado establecerá que todos los empleados con acceso o que participen en el tratamiento de datos personales deben de haber realizado la formación. El procedimiento proporciona dos vías para la formación: recursos abiertos (para los que se proporcionan algunos materiales como referencia), cursos de formación externos y los requisitos mínimos que estos deben contener en su temario. Finalmente, el procedimiento detallará dos métodos de evidencia, en función de cuál haya sido la ruta formativa escogida, bien declaración responsable firmada por empleado y responsable del tratamiento, bien certificado emitido por la empresa que imparta el curso y que acredite la asistencia del empleado.

- Registro de actividades de tratamiento: este procedimiento se centra en definir el contenido mínimo que los registros de actividades de tratamiento deben tener. Además, buscará enumerar a forma de guía valores aceptables para los distintos elementos: tipo de datos, finalidades, categorías, bases legitimadoras… Estas enumeraciones no contendrán todas las posibilidades (en algunos casos la lista es prácticamente ilimitada). El diseño de este documento se basa principalmente en las definiciones del Reglamento General de Protección de Datos (8) y la información proporcionada en la plantilla de ejemplo creada por la autoridad de control francesa (CNIL) (27).

- Análisis del riesgo y evaluación de impacto: como ya se ha mencionado en secciones anteriores, el análisis de riesgos puede llegar complejo cuando se requiere un análisis formal siguiendo una metodología definida. Sin embargo, para los casos más básicos es posible la realización de un análisis ad-hoc bastante simplificado. Este procedimiento describirá los requisitos que el análisis básico debe cumplir. También deberá dejar claro en qué casos no será suficiente y se deberá recurrir a ayuda externa para realizar el análisis formal y la evaluación de impacto correspondiente. Finalmente, aunque para el análisis de riesgos básico no se requiere seguir ninguna metodología concreta, se tomarán como referencia las propuestas de CNIL, la AEPD y ENISA (20, 22, 28).

- Medidas de técnicas seguridad: el conjunto de medidas de seguridad aplicables es bastante extenso y depende fuertemente del análisis de riesgos. No obstante, hay una serie de medidas que son recomendables independientemente del resultado del

análisis de riesgos. Se está pensando en medidas que se aplicarían incluso en situaciones de riesgo bajo. Por ejemplo, contraseñas seguras, controles de acceso, autenticación de usuarios, cifrado de comunicaciones… Este tipo de medidas se pueden encontrar como ejemplo en (20, 22). También se desarrollará una normativa que incluya todas las medidas propuestas, explicando los requisitos que deben cumplir (por ejemplo, longitud de contraseñas). Finalmente, se incluirá un procedimiento de gestión de incidentes que describirá como debe actuarse en casos de filtraciones de datos personales o en la materialización de amenazas que afecten a la continuidad del negocio y, por tanto, a la disponibilidad de los datos personales. Para ello se tomarán como referencia las guías de CNIL y AEPD (22, 29).

- Consentimiento: este procedimiento se centra en establecer los requisitos con los que debe contar el consentimiento según lo establecido por la regulación (8, 9). Entre estos requisitos destacarán los textos legales que deben acompañar a toda solicitud de consentimiento. Para esto último, se utilizarán los ejemplos proporcionados por la herramienta FacilitaRGPD[15].

- Ejercicio de derechos: es uno de los aspectos más complejos a la hora de garantizar el cumplimiento de la normativa. Para desarrollar el procedimiento asociado a este punto, tomamos como referencia los procedimientos de la Universidad Politécnica de Valencia y la LSE (London School of Economics) (30, 31). Siguiendo las referencias aportadas, desarrollaremos un diagrama de flujo del proceso y documentaremos los requisitos específicos de cada derecho como la identificación del interesado entre otros. Finalmente, utilizaremos los formularios de solicitud proporcionados por la Agencia Española de Protección de Datos: acceso[16], rectificación[17], supresión[18], oposición[19], portabilidad[20] y limitación[21].

- Contrato de encargado: el contrato de encargado de tratamiento es un documento altamente dependiente de las condiciones del tratamiento que se realice sobre los datos. No obstante, la legislación (8, 9) establece unos requisitos mínimos que deben ser cumplidos. Estos requisitos se incluirán en nuestro procedimiento de creación de contratos de encargado de tratamiento que, a su vez, se incluirán como clausulas en los contratos que se firmen. Estas cláusulas utilizarán como referencia las propuestas por la AEPD en (32) y las cláusulas tipo establecidas por la Comisión Europea (33, 34). Además, se incluirá la opción de establecer relaciones con encargados de tratamiento que se adhieran al código de conducta de la autoridad de control o que cuenten con una certificación en el RGPD.

- Delegado de protección de datos: el delegado de protección de datos no es un elemento necesario para todos los negocios. El procedimiento deberá de aportar la

[15] Facilita AEPD. https://facilita.aepd.es

[16] Formulario derecho de acceso. https://www.aepd.es/documento/formulario-derecho-de-acceso.pdf

[17] Formulario derecho de rectificación. https://www.aepd.es/documento/formulario-derecho-de-rectificacion.pdf

[18] Formulario derecho de supresión. https://www.aepd.es/documento/formulario-derecho-de-supresion.pdf

[19] Formulario derecho de oposición. https://www.aepd.es/documento/formulario-derecho-de-oposicion.pdf

[20] Formulario derecho de portabilidad. https://www.aepd.es/documento/formulario-derecho-de-portabilidad.pdf

[21] Formulario derecho de limitación https://www.aepd.es/documento/formulario-derecho-de-limitacion.pdf

mayor claridad posible sobre cuando es un requisito indispensable para el negocio. En el caso en el que un delegado sea requerido, el procedimiento establecerá los requisitos mínimos que debe cumplir y que evidencias deben recogerse. La autoridad de control española (AEPD) ha creado una certificación específica (35) para identificar delegados de protección de datos que cumplen los requisitos mínimos. Sin embargo, el porcentaje de delegados certificados frente al total es bajo (ver Figura 3).

Figura 3. Delegados de protección de datos certificados con respecto al total. Fuente: AEPD[22]

El diseño del apartado de registros será ligeramente diferente. En algunos casos concretos; por ejemplo, para el registro de actividades de tratamiento, se incluirá también una plantilla. No obstante, el diseño de los registros se centra más en cómo organizar las evidencias de una forma sencilla y en la nomenclatura de estos, haciendo especial énfasis en resaltar las fechas en las que las evidencias fueron tomadas. Revisemos a continuación el diseño punto por punto:

- **Formación:** el registro de la formación es bastante sencillo, contendrá una carpeta por cada empleado. En la carpeta de empleado se almacenará, bien el certificado del curso realizado (si esta fue la opción escogida) o de la declaración responsable (en caso de formación usando materiales formativos abiertos). Se propone una carpeta por empleado como método de organización ya que puede haber más de una formación durante el periodo de pertenencia a la empresa.

- **Registro de actividades de tratamiento:** se proporcionará una plantilla con los campos necesarios, tal y como se han definido el procedimiento. La plantilla utilizada será la proporcionada por CNIL (27), traducida y adaptada al caso que nos ocupa. La idea principal es que exista una carpeta para cada actividad de tratamiento que, además del registro, contenga toda la información necesaria para localizar los datos involucrados (si se considera necesario).

- **Análisis del riesgo y evaluación de impacto:** el registro para el análisis de riesgos contará con un único documento que contendrá lo necesario para satisfacer los requisitos impuestos por el procedimiento.

- **Medidas de seguridad:** al igual que para los procedimientos asociados, se propone la creación de carpetas (una por cada medida) que contendrán las evidencias o, en su caso, las indicaciones para poder evidenciar la implantación de una medida. Por ejemplo, para demostrar que se cumplen las políticas de contraseñas, se podría almacenar una captura de pantalla de la configuración o las instrucciones sobre cómo llegar al panel de configuración.

[22] Agencia Española de protección de datos (AEPD). https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion

- **Consentimiento:** siempre que recojamos el consentimiento deberemos almacenarlo como evidencia. Los registros se organizarán de la siguiente manera. Crearemos una carpeta por cada actividad de tratamiento que, a su vez, contendrá una carpeta por interesado que almacenará el histórico de consentimientos (habrá histórico en aquellos casos en los que se requiera otorgar de nuevo el consentimiento). Habrá otros casos en los que el consentimiento se encuentre almacenado directamente en otro sistema, en esos casos podremos crear un documento (un bloc de notas, por ejemplo) que indique donde se almacenan los consentimientos o almacenar una copia del almacén del sistema original.

- **Ejercicio de derechos:** el registro del ejercicio de derechos contará con una carpeta para cada derecho. A su vez, cada una de estas contará con una carpeta para cada interesado. Finalmente, se creará un nivel más (una nueva carpeta) por cada solicitud ya que se almacenarán todas y cada una de las solicitudes realizadas por cada interesado. Los objetivos de este último nivel son: almacenar la solicitud recibida, almacenar evidencias del procesamiento de la solicitud y almacenar la respuesta proporcionada al interesado

- **Contrato de encargado:** este registro constará de una carpeta por cada encargado, que contendrá el contrato suscrito y todos los documentos que se hayan proporcionado como evidencia para cumplir con lo establecido en el contrato.

- **Delegado de protección de datos:** la recogida de evidencias para este aspecto es sencilla. Crearemos una carpeta para cada delegado. Al principio solo habrá uno, pero se debe tener en cuenta que en algún momento se producirá un cambio de delegado. Esta carpeta contendrá todas las evidencias necesarias para probar que el delegado cumple con los requisitos mínimos o el certificado emitido por una certificadora autorizada, en su caso.

4.3 Tecnología utilizada

Para la realización de este trabajo se han utilizado múltiples herramientas y tecnologías. Se han utilizado las herramientas de ofimática: Word y Excel como medios principales para el desarrollo de todos los documentos que forman parte del sistema de gestión. Otra tecnología fundamental utilizada, es la estructura organizativa en carpetas que proporcionan los sistemas de archivos. Esta tecnología, además de proporcionar una estructura organizativa, nos permite establecer permisos específicos para cada carpeta. Esta funcionalidad es esencial en el caso de que queramos limitar el acceso a alguna de las partes del sistema de gestión. Por ejemplo, pongamos que un empleado se encarga de almacenar los consentimientos obtenidos. Sin embargo, el propietario del negocio no quiere que sus empleados conozcan los términos exactos de los contratos de encargado de tratamiento. En este caso los permisos son un elemento más del sistema que nos permite realizar un control de acceso.

Otra parte necesaria para la realización de este trabajo es la definición de procesos complejos que deben llevarse a cabo para cumplir con la normativa de protección de datos. Para plasmar estos procesos de forma sencilla y comprensible se han utilizado diagramas de flujo y la notación BPMN 2.0. Existen multitud de herramientas para la creación de los diagramas. Para el desarrollo de este trabajo decidimos utilizar Lucidchart, una plataforma de creación de todo tipo de diagramas (UML, flujo, red…) que se oferta en un modelo de plataforma como servicio (SaaS) y permite su uso gratuito para diagramas de tamaño reducido.

También se utilizaron otras herramientas propias de la gestión de proyectos y el análisis de negocio. En concreto, utilizamos diagramas de Gantt para la definición de la expectativa temporal del desarrollo de las tareas a realizar. Esta herramienta permite además analizar el camino crítico y definir el riesgo de las tareas, de esta forma es posible analizar si existe el riesgo de que se alarguen los plazos. Finalmente, se utilizaron herramientas como el análisis de riesgos y las matrices probabilidad impacto. Estas herramientas son esenciales para la definición del análisis de riesgos requerido por la norma, por lo que su uso, es una de las partes más importantes para la construcción del sistema de gestión.

5 Desarrollo de la solución propuesta

En esta sección revisaremos los aspectos fundamentales del sistema de gestión desarrollado. Aunque se muestran varios aspectos generales del sistema, no se pretende llevar a cabo una revisión pormenorizada. Por tanto, puede haber aspectos menos importantes, pero aun así relevantes que no hayan sido incluidos.

La plantilla desarrollada cuenta con tres elementos fundamentales: portada, índice de contentido y cajetín de versionado. La portada muestra el título de documento y la fecha del documento, que deberá coincidir con la feha de aprobación de la última modificación. El índice de contenido muestra los elementos fundamentales que deberán contener todos los procedimientos: una sencilla introducción que aporte el contexto para comprender el contenido, los objetivos que el procedimiento pretende desarrollar, el propio contenido, el histórico de versiones del documento y las referencias utilizadas en la construcción del procedimiento. Finalmente, merece la pena destacar el cajetín de versionado como un elemento fundamental para la gestión de cambios del procedimiento. Este cajetín establece elementos fundamentales como: la versión del documento, los cambios asociados a una versión concreta, el autor de las modificaciones, el responsable de revisar y aprobar las modificaciones realizadas y, finalmente la fecha aprobación de las modificaciones.


PROCEDIMIENTO
TÍTULO DEL PROCEDIMIENTO

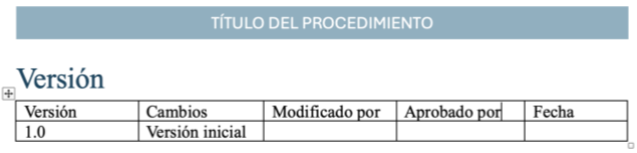
FECHA: DD/MM/AAAA

Figura 4. Portada de la plantilla de procedimientos


TÍTULO DEL PROCEDIMIENTO

Tabla de contenido

Figura 5. Índice de contenido de la plantilla de procedimientos


TÍTULO DEL PROCEDIMIENTO

Versión

Versión	Cambios	Modificado por	Aprobado por	Fecha
1.0	Versión inicial			

Figura 6. Cajetín de versionado de la plantilla de procedimientos

Un análisis de riesgos puede llegar a ser un proceso muy complejo dada la enorme cantidad de amenazas a considerar, el número de dimensiones de evaluación del riesgo, la ambigüedad de la determinación de los niveles de impacto y probabilidad, etc. En un intento de sortear estas dificultades se ha desarrollado un procedimiento que intenta definir, de la forma más clara posible, todos los elementos necesarios. Mediante la utilización de Tabla 1 y las definiciones del procedimiento para cada uno de los elementos la determinación del riesgo se simplifica enormemente. Para cada par actividad-amenaza se determina un nivel de impacto y una probabilidad, dando lugar al nivel de riesgo correspondiente a tratar.

Probabilidad	Alta	Medio	Alto	Muy alto	Muy alto
	Media	Medio	Medio	Alto	Muy alto
	Baja	Bajo	Medio	Medio	Alto
	Improbable	Bajo	Bajo	Medio	Medio
		Muy limitado	Limitado	Significativo	Muy significativo
		Impacto			

Tabla 1. Matriz probabilidad-impacto. Fuente: Elaboración propia partiendo de (28).

Uno de los procesos fundamentales para el cumplimiento de la normativa en vigor de protección de datos personales, es el ejercicio de derechos por parte de los interesados. Estos derechos proporcionan una herramienta para el control efectivo de las actividades de tratamiento que los utilizan. Este proceso es de los más complejos que se deben llevar a cabo para el mantenimiento del sistema de gestión desarrollado. Esto se debe a que cada derecho se puede ejercitar bajo una serie de supuestos distintos y cada uno debe seguir un procedimiento distinto. No obstante, todos ellos comparten un proceso común previo y posterior a la tramitación especifica. Por ello, se desarrolló un diagrama de flujo para el proceso común con el objetivo de establecer un proceso repetible y sencillo.

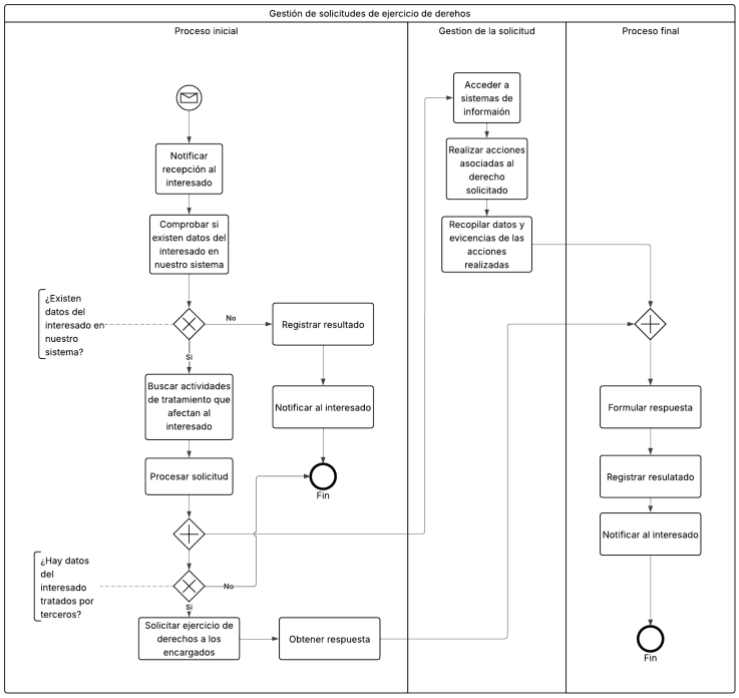


Figura 7. Proceso general para la gestión de solicitudes de derechos

6 Implantación

El sistema desarrollado en este trabajo debe ser implantado en un negocio real para poder demostrar su utilidad. Para ello se incluye en este apartado una metodología de implantación. Esta metodología definirá el orden que se debe seguir para pasar de un estado de cero cumplimiento a la integración total de los procesos del sistema de gestión en el día a día del negocio. La metodología desarrollada considerará dos escenarios: implantación desde cero y transición desde la antigua legislación de protección de datos (4).

El escenario de implantación desde cero nos sitúa en una empresa que prácticamente no realiza ningún tratamiento de datos personales. Para evitar las dificultades que entraña tratar datos de carácter personal, este negocio ha decidido no realizar ningún tipo de tratamiento más allá de los esenciales (laboral, fiscal…) que deriva íntegramente en una gestoría.

El segundo escenario se aplica a un negocio que realiza tratamientos de datos personales conforme a la legislación antigua. Esta situación puede deberse, por un lado, a que el negocio no conoce la existencia de la nueva legislación (8, 9) y piensa que aquello con lo que cuenta es más que suficiente. O, por otro lado, y pese a conocer la existencia de una nueva legislación, considera que los cambios son menores y decide no llevar a cabo una revisión de sus procesos. En cualquier caso, el proceso general de implantación será el mismo. Aunque habrá que matizar que, en aquellos casos en los que exista un tratamiento previo, podrá ser necesario llevar a cabo cierto tipo de acciones especiales. Por ejemplo, puede ser necesario volver a solicitar el consentimiento para adaptarlo a la nueva regulación.

El proceso general de implantación está definido con una estructura y un orden que coincide con el diseñado para el sistema de gestión, de esta forma es muy sencillo relacionar los conceptos con el proceso. Además, esta forma de proceder nos permite ir revisando uno a uno los procedimientos modelo proporcionados e ir adaptándolos a las necesidades del negocio conforme se implanta el sistema. A continuación, se describen las fases de implantación:

1. **Formación:** la formación del personal del negocio es el primer paso que debe darse a la hora de implantar el sistema. Se requiere tener unos conocimientos mínimos, si no, será imposible realizar una identificación fiable de datos personales, actividades de tratamiento… El punto más importante de la formación debería ser la capacidad de identificar correctamente cuando estamos ante un dato personal, ya que de ello depende poder aplicar correctamente la normativa. Realizada la formación solo queda recoger las evidencias, es decir, solicitar certificados de asistencia o firmar declaraciones responsables.

2. **Identificación de actividades de tratamiento:** el primer paso tras la formación debe ser, sin duda alguna, la identificación de las actividades de tratamiento y todo lo relacionado con ellas. Todos los pasos posteriores partirán de los resultados de esta tarea. Dada la importancia de esta tarea y de los diferentes elementos que la contienen. Se decide que es necesaria una subdivisión en distintas sesiones, cada una orientada uno de los aspectos fundamentales de las actividades de tratamiento:

    a. **Identificación de los datos personales y las categorías asociadas:** este punto bebe directamente de la formación recibida en la primera sesión de implantación. Se deberán utilizar los ejemplos del procedimiento de actividades de tratamiento para identificar todos los datos personales que son tratados en el negocio, independientemente de su origen o ámbito. Si el dato personal se utiliza en el negocio, debe ser incluido. También es importante saber en qué procesos se utiliza. Además, se categorizarán

estos datos utilizando también las categorías incluidas en el procedimiento como guía. Por ejemplo, datos de clientes, proveedores, datos financieros, de salud, de identificación…

b. **Identificación de bases legitimadoras, finalidades y periodos de retención:** en esta sesión se deberán agrupar los datos en actividades de tratamiento diferenciadas (un dato personal puede utilizarse en varias actividades de tratamiento). Por lo general, una actividad de tratamiento tendrá una única finalidad, esta forma de diferenciación nos permitirá una gestión más sencilla de los procesos del sistema. Seguidamente, deberemos identificar cuáles son las bases legitimadoras que soportan las actividades de tratamiento. Finalmente, identificaremos cual es el periodo de retención asociado a las actividades de tratamiento. En el caso en el que se estén tratando datos para los que la base legitimadora sea el consentimiento y estos se hubieran obtenido con la legislación previa (consentimiento tácito), será necesario identificar si existe alguna base legitimadora para continuar el tratamiento o es necesario solicitar el consentimiento explícito. En cualquier caso, será necesario notificar a los interesados.

c. **Identificación de cesiones de datos, transferencias internacionales, encargados de tratamiento:** conocidas las actividades de tratamiento, pasamos a identificar si esos datos se trasmiten a terceros y en qué condiciones. Deberemos identificar, para cada actividad de tratamiento, si los datos se ceden a terceros, medie contraprestación económica o no. También identificaremos si los datos se ceden a terceros para realizar un tratamiento a cuenta del responsable (por ejemplo, a una gestoría). Finalmente, deberemos identificar si en cualquiera de las cesiones anteriores se traspasan las fronteras del país. En caso afirmativo, deberemos identificar a que países se transmiten los datos; si esta transferencia puede ser amparada por algún acuerdo; o si esa transferencia debe ser evitada.

d. **Identificar oportunidades de aplicación de los principios de diseño:** llegados a este punto, conocemos todo lo relativo a las actividades de tratamiento de datos personales que se realizan en el negocio. Por tanto, es un buen momento para revisar que las actividades cumplen con los principios de diseño. ¿Se han obtenido todos los datos de forma licita? ¿Existe algún dato personal que no sea necesario? ¿El plazo de conservación es razonable?

e. **Crear el registro de actividades de tratamiento:** tras todo el análisis anterior es momento de plasmarla en el registro. Para ello crearemos una copia de la plantilla para cada actividad de tratamiento y rellenaremos todos los campos con la información necesaria.

3. **Análisis de riesgos y análisis de impacto:** el análisis de riesgos es una de las fases potencialmente más compleja del proceso de adecuación. Sin embargo, esto no es así en todos los casos. Existen casos (principalmente si el riesgo del tratamiento es bajo) en los que bastará con la realización de un análisis básico prácticamente al alcance de cualquiera. Por tanto, lo primero será determinar si es necesario realizar un análisis formal y basado en una metodología reconocida, además de una evaluación de impacto. En caso afirmativo, la recomendación es

subcontratar este proceso a una empresa externa que se especialice en este punto. Si, por el contrario, decidimos realizar nuestro propio análisis de riesgos básico el proceso de implantación que proponemos es el siguiente:

a. **Identificar de activos y amenazas:** para realizar un análisis de riesgos es necesario conocer los activos que son susceptibles de ser vulnerados y que, en consecuencia, supongan un riesgo en el tratamiento de datos personales. Una gran parte de este trabajo ya se ha realizado durante el establecimiento del registro de actividades de tratamiento. En aquella fase de la implantación se identificaron los datos personales tratados, así como quién o qué tiene acceso a ellos. Esta fase requerirá profundizar en la identificación de todos los activos relacionados con el tratamiento de datos personales. El primer activo es el dato personal. Todo dato personal es tratado en un lugar, por una o más personas y mediante un soporte informático (salvo que el tratamiento se realice en papel). Una vez identificados los activos, será necesario identificar las amenazas a las que estos están sometidos. Por ejemplo, un ordenador puede ser hackeado, puede dejar de funcionar, etc. El factor humano también debe ser tenido en cuenta. Un empleado puede cometer un error, ser sobornado, etc. Finalmente, una ubicación física puede sufrir robos, perdida del suministro eléctrico, inundaciones, etc. La identificación de amenazas es clave para poder evaluar el riesgo.

b. **Evaluación del riesgo sobre los activos:** en la fase anterior identificamos los activos y las amenazas a las que están expuestos. Con esa información es posible, mediante el establecimiento de una metodología probabilidad-impacto, identificar el nivel de riesgo al que está expuesto un activo. El procedimiento de análisis de riesgos establece los niveles cualitativos de evaluación del impacto y del riesgo. También establece cual es el nivel de riesgo aceptable. Con todo lo anterior asignaremos a cada par actividad-amenaza una valoración de impacto y una valoración de probabilidad. Como resultado obtendremos un nivel de riesgo concreto que nos permitirá comparar con el umbral de riesgo aceptable. Si dicho umbral es superado será necesario establecer una medida de seguridad que rebaje el nivel de riesgo. Por tanto, el resultado final de esta fase será, por un lado, el registro de análisis de riesgos y, por otro, las medidas de seguridad que será necesario implementar.

4. **Implantación de medidas de seguridad:** las medidas de seguridad son un elemento fundamental para mitigar riesgos y garantizar la seguridad de los datos personales. Para implementarlas realizaremos las siguientes tareas:

a. En la fase anterior se obtuvieron las medidas de seguridad necesarias para mitigar los riesgos detectados. A ese conjunto de medidas añadiremos aquellas que se consideren necesarias. Algunas de estas medidas serán requisitos establecidos por las autoridades de control por ser consideradas buenas prácticas o indispensables para la seguridad de los datos personales, por ejemplo, establecer contraseñas complejas. En caso de existir medidas de seguridad ya implementadas, habrá que comprobar si son suficientes o requieren de algún ajuste. Siguiendo con el ejemplo anterior, una política de contraseñas existente pero no lo suficientemente compleja. Llegados a este punto solo nos queda decidir qué medidas pueden ser implantadas directamente por los empleados de

la organización, y para qué medidas se necesita de ayuda de un profesional especializado dada su complejidad.

b. **Implantación de medidas:** una vez se ha decido quién será el encargado de la implantación de las medidas, solo queda proceder a su implantación. La parte más importante de esta tarea, además de la propia implantación, es la recogida de evidencias. Para cada medida implantada se deberá poder comprobar que está activa. Para ello, podremos almacenar documentos (capturas de pantalla, ficheros…) que evidencien lo que se afirma o instrucciones que proporcionen los pasos necesarios a realizar para verificar que la medida está implantada correctamente. Por ejemplo, podríamos acceder al panel de control para comprobar que las políticas de contraseña establecidas se corresponden con los requisitos mínimos exigidos.

5. **Gestión de consentimientos:** una gran parte del trabajo para iniciar la gestión de consentimientos ya fue realizada durante la definición de actividades de tratamiento. En esta fase de la implantación deberemos incorporar dicha información:

    a. **Analizar el cumplimiento de datos existentes:** partiendo del análisis realizado en la fase 2.b comprobaremos que consentimientos es necesario actualizar, si los hay.

    b. **Definir consentimiento para las actividades de tratamiento:** para cada actividad de tratamiento cuya base legitimadora sea el consentimiento, deberemos generar un texto legal que cumpla los requisitos establecidos en el procedimiento de gestión de consentimiento.

    c. **Incorporar consentimientos existentes:** para aquellos consentimientos que existan antes de la implantación de este sistema de gestión, deberemos incorporarlos, incluyéndolos en la carpeta de registros del grupo 5. Gestión del consentimiento. Si existen consentimientos en papel, es conveniente escanearlos e incorporarlos al sistema de forma digital.

    d. **Recabar el consentimiento renovado:** en el caso en el que se hayan identificado consentimientos que deben ser renovados, deberemos decidir si se comunica con los interesados para solicitar de nuevo el consentimiento o se renuncia a continuar con el tratamiento de esos datos. En el caso de obtener el consentimiento explícito de los interesados contactados se incorporarán como evidencia, al igual que cualquier otro consentimiento.

6. **Gestión de derechos:** la fase de implantación del proceso de gestión de derechos es bastante sencilla. La complejidad llegará cuando se reciban solicitudes. Sin embargo, es complicado realizar una preparación previa más allá de la gestión que se pueda hacer de solicitudes simuladas para practicar los procesos:

    a. **Revisión de procesos:** esta fase es sin duda la más importante. Se procederá a analizar si el proceso establecido en el procedimiento proporcionado como modelo se adapta correctamente a las necesidades del negocio. Una vez completado este análisis es recomendable realizar

la gestión simulada de solicitudes. Esta simulación tiene como objetivos validar el proceso diseñado y que el personal implicado en la gestión de los derechos interiorice el proceso y lo lleve a cabo de manera sistemática.

b. **Incorporar solicitudes existentes al sistema:** es posible que, de forma previa a la implantación del sistema, se hayan recibido solicitudes de ejercicio de derechos. Independientemente de que la gestión pasada se ajuste al nuevo sistema es necesario incorporar toda evidencia del procesamiento de dichas solicitudes.

7. **Contratos de encargado de tratamiento:** esta fase consistirá en la revisión de todos los contratos de encargado existentes si los hubiera. También se tomarán las acciones necesarias para actualizarlos de forma que cumplan con la normativa.

    a. **Analizar contratos existentes:** es bastante probable que existan contratos de encargado de tratamiento para los servicios externalizados que traten datos personales. En ese caso será necesario revisar las cláusulas para comprobar que cumplen con los requisitos definidos en el procedimiento 7. No es necesario que existan todas las cláusulas una a una, será suficiente con asimilarlas a alguna de las definidas en el procedimiento (si es posible).

    b. **Adaptar contratos a la normativa:** si en la fase anterior se han identificado cláusulas no incluidas, será necesario contactar con los encargados y modificar el contrato o incluir una adenda. Hay que tener en cuenta que este proceso no siempre será sencillo. Puede haber algún encargado que se niegue a cumplir con alguno de los requisitos. En esos casos será necesario tomar medidas para garantizar el cumplimiento. Se podría limitar los datos personales tratados (si es posible) para intentar reducir las exigencias que se trasladan al encargado. Sin embargo, es posible que haya ocasiones en las que sea necesario cambiar a un proveedor que esté dispuesto a cumplir con los requisitos para garantizar la seguridad del tratamiento de datos personales.

8. **Delegado de protección de datos:** en la mayoría de los casos, no será necesario contar con un delegado de protección de datos. Por lo tanto, esta fase de la implantación se reduce a, siguiendo el procedimiento, determinar si existe la necesidad de un delegado de protección de datos y, en caso afirmativo, a proceder a su contratación.

9. **Revisión periódica del sistema:** finalmente, es necesario establecer un proceso de revisión interna con cierta periodicidad. Este proceso, que se iniciará al terminar la implantación del sistema, nos permitirá revisar el cumplimiento de manera periódica. La idea subyacente es que siempre es posible pasar ciertos aspectos relevantes por alto, o que se produzcan cambios relevantes que no se incorporen al sistema. Este proceso de revisión nos permitirá tener controladas ambas situaciones y mantener el sistema de gestión actualizado. La periodicidad de estas revisiones puede ser mensual, trimestral, semestral o anual. En cualquier caso, la periodicidad se ajustará al ritmo de cambio que se produzca en las actividades de tratamiento. Si prácticamente no se producen cambios, la periodicidad anual será más que suficiente. Por el contrario, si los cambios son

frecuentes, será necesario incrementar la periodicidad con la que se revisa el sistema. Estas revisiones deberían realizarse por escrito, se pueden evidenciar con un acta de la reunión en la que se realiza la revisión. Esta acta documentará las deficiencias halladas (si las hay) y propondrá soluciones que deberán incorporase al sistema antes de la próxima revisión. Finalmente, es recomendable contratar auditorías externas con periodicidad anual/bianual. Estas auditorias son similares a las revisiones internas, pero se realizan por personal ajeno a la empresa. Además, permiten ir un paso más allá y proporcionar la certificación de cumplimiento de la normativa de protección de datos si así se desea, aunque siempre habrá considerar los costes económicos asociados.

A continuación, se han incluido los diagramas Gantt con las tareas a realizar y la duración esperada para cada una de ellas. Hay tres niveles de riesgo aplicados sobre las tareas: bajo, medio y alto. El nivel bajo está destinado a tareas sencillas y que no deberían de extenderse más allá del tiempo previsto. El nivel medio está destinado a tareas complejas que dependen exclusivamente del responsable del tratamiento, por lo que no deberían de superar el tiempo previsto salvo en casos específicamente complejos. Finalmente, el nivel alto se asigna a tareas que implican a actores externo y, en consecuencia, son susceptibles de extenderse en el tiempo por diversos motivos.

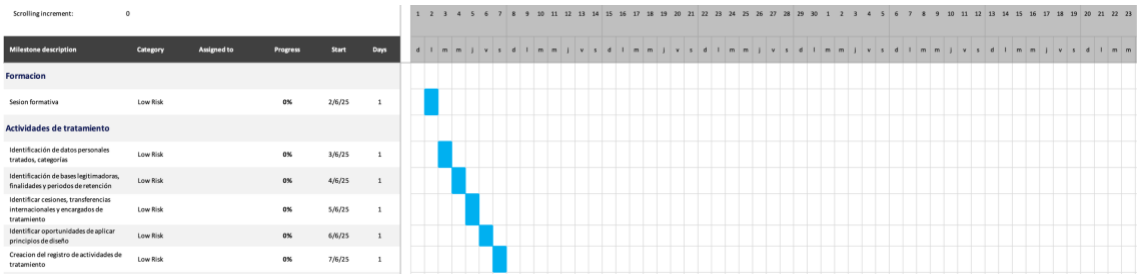


Figura 8. Diagrama de Gantt de las dos primeras fases del proceso de implantación.[23]

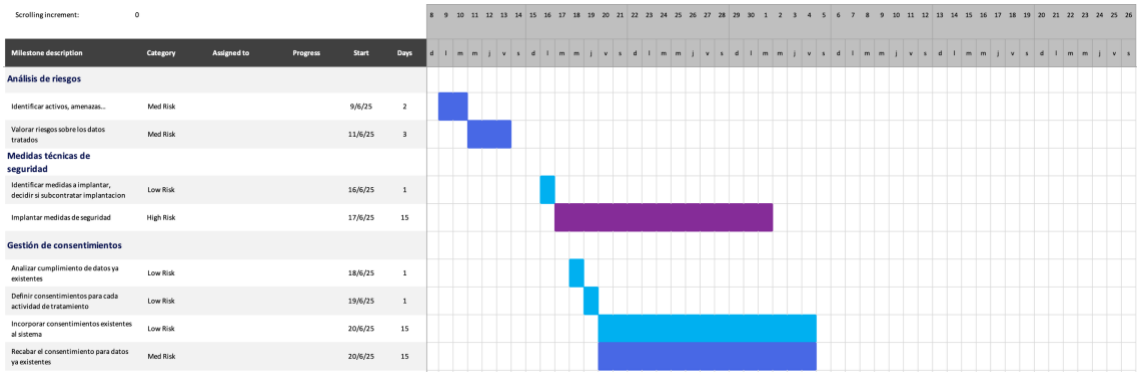


Figura 9. Fases intermedias: análisis de riesgos, medidas de seguridad y gestión de consentimientos.[23]

[23] Plantilla Agile Gantt Chart. https://create.microsoft.com/en-us/template/agile-gantt-chart-c29ed7ae-85bf-4494-9a46-cf50fab44efa

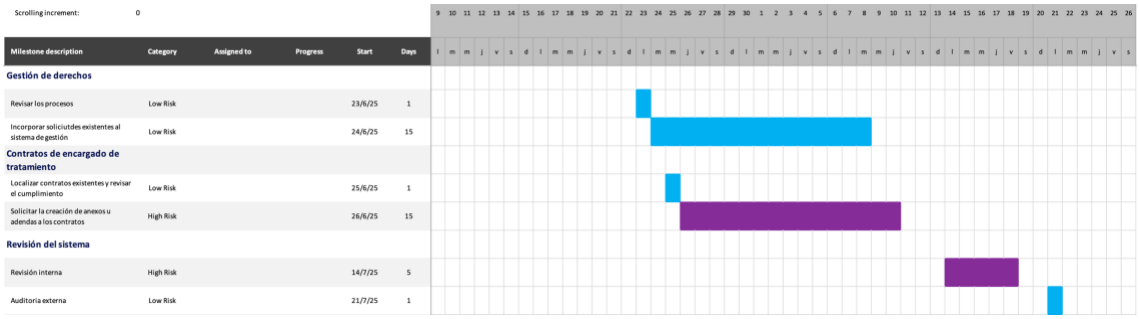


Figura 10. Fases finales: gestión de derechos, contratación de encargados de tratamiento y revisión final.[23]

6.1 Casos prácticos

Pese a que hemos definido una metodología de implantación, este trabajo no llegó a aplicarla en un pequeño comercio. No obstante, en un intento de mitigar esta deficiencia, se propone la creación de 4 casos ficticios basados en nuestro conocimiento del pequeño comercio. Es cierto que aquello que podamos saber sobre las actividades de estos negocios, no llegará a hacer justicia a sus realidades operativas. Sin embargo, aportando casos prácticos concretos podemos llegar a construir una suerte de guía que ayude a resolver las dudas más frecuentes. A continuación, construiremos los cuatro comercios que servirán de ejemplo:

- Farmacia S.L: este negocio es una farmacia que lleva en el barrio varios años. Por tanto, conoce a los clientes habituales y sus empleados suelen realizar recomendaciones sobre nuevos productos que llegan al mercado como cremas u ofrecer servicios como la toma de tensión arterial. Pese a que están bastante contentos, les gustaría extender este sistema para realizar recomendaciones en base a los medicamentos comprados en el pasado por sus clientes. Por supuesto, este caso involucra otro tipo de regulaciones de índole sanitaria, pero supondremos que todo lo externo a lo relacionado con la protección de datos se realiza conforme a la legislación vigente.

- Restaurante S.L: Este negocio es un restaurante que lleva abierto más de 15 años. Recientemente ha sido objeto de un cambio de titularidad, por compraventa. Su dueño ha decidido jubilarse. Además, cuenta con un moderno sistema de reservas online recientemente implantado. El negocio cuenta con página web que integra el sistema de reservas.

- Zapatería S.L: Este negocio es un pequeño comercio con más de 30 años a sus espaldas. La empresa forma parte del grupo empresarial Grupo S.A junto con otro negocio, Tintorería S.L. Zapatería S.L cuenta con una página web y vende sus productos en Amazon.

- Tintorería S.L: Este negocio, de reciente creación, forma parte del mismo grupo empresarial que Zapatería S.L. Su propietario decidió crear Grupo S.A en lugar de registrar una nueva actividad y modificar la marca Zapatería S.L. Tintorería S.L cuenta con página web y, al ser un negocio nuevo, se involucrará en actividades de captación de clientes.

A continuación, se aplica la metodología de implantación a los casos prácticos:

6.1.1 Formación

Se presupone realizada. Por tanto, no se incluye caso práctico ya que no hay nada destacable que resaltar en este apartado

6.1.2 Actividades de tratamiento

Comenzamos suponiendo que las siguientes actividades de tratamiento son comunes a todos los negocios: gestión laboral, gestión de candidatos, gestión de proveedores, gestión de clientes (fiscal), videovigilancia del local. Además, todas las actividades de tratamiento que se tratan en estos ejemplos son continuadas en el tiempo, (no son temporales) por lo que será necesario incluirlas en el registro de actividades del tratamiento.

La actividad de gestión laboral consiste en todo tratamiento de datos necesario para realizar todas las tareas asociadas a: contratos, cumplimiento legislación laboral, gestión de salarios, etc. Este tratamiento se basa en la necesidad de datos para la ejecución de contratos y la necesidad del cumplimiento de obligaciones legales, por lo que no hace falta consentimiento. En general, no se tratarán datos considerados sensibles (datos de salud, ideología…). Suponemos que esta gestión la realizará una gestoría, por lo que será necesario el establecimiento de un contrato de encargado de tratamiento. No se realizan cesiones de datos a terceros (a excepción de la gestoría) ni transferencias internacionales de datos. Finalmente, el periodo de retención de los datos será el mismo que la duración del contrato, además de los 5 años de conservación necesarios tras la finalización de la relación laboral (por imperativo legal). Se deberá informar a la gestoría de todas las actividades de monitorización de empleados: videovigilancia, monitorización de ordenadores, etc. Finalmente, todos los contratos laborales incluirán el texto legal informado a los interesados de todo lo anterior, incluyendo lo relativo al ejercicio de derechos.

La actividad de gestión de candidatos consiste en el tratamiento de datos para la selección de personal. Los datos personales involucrados serán aquellos incluidos en el currículum. Este tratamiento se basa en el consentimiento. Los currículums serán almacenados durante la duración del proceso de selección (se pueden conservar más tiempo si así se decide). Si el proceso de selección se externaliza hará falta un contrato de encargado de tratamiento, en un sentido u otro dependiendo de quien recoja los datos. No hay cesiones a terceros ni transferencias internacionales de datos. Finalmente, se informará a los interesados de los derechos que pueden ejercer (en este caso el más común será el de supresión, generalmente retirando el consentimiento).

La actividad de gestión de proveedores consiste en el tratamiento de datos relativos a los contratos con proveedores. Generalmente, la mayoría de los datos relativos a proveedores son los pertenecientes a entidades con personalidad jurídica y quedan fuera de la legislación de protección de datos. Sin embargo, en estas relaciones también se intercambiarán datos relativos al personal del proveedor. Estos tratamientos se basan en la relación contractual, puede haber cesiones a encargados de tratamiento como una gestoría. En general, no habrá transferencias internacionales. El periodo de retención será igual a la duración del contrato, sumado al periodo de retención legal tras la finalización de la relación contractual, por imperativo legal.

La actividad de gestión de clientes en lo relativo a las obligaciones fiscales consiste en la gestión de facturación. Los clientes pueden solicitar una factura y, en esos casos, deberán aportar datos personales: nombre, NIF, dirección, etc. Este tratamiento se basa en el cumplimiento de la legislación. En general, no habrá transferencias internacionales. No obstante, si se usa una gestoría se producirá una cesión bajo un contrato de encargado de tratamiento. Finalmente, el periodo de retención será de 4 años, por imperativo legal.

En lo relativo a la gestión de la facturación cabe señalar que hemos obviado el contenido de la factura como dato tratado. En algunos casos, Farmacia S.L, la factura puede incluir datos relativos a la salud (consumo de medicamentos de los que se pueden inferir patologías concretas).

Es muy importante no incluir estos datos a la gestoría, esta cesión es totalmente innecesaria y no está amparada por la base legitimadora utilizada.

El último caso común abordado será la videovigilancia del interior del local. La finalidad de esta actividad es la protección de los bienes del local, evitar robos, daños… Los datos recogidos serán los relativos a la imagen de las personas que entren en las instalaciones. Esta actividad se basará en el interés legítimo[24], no se realizarán cesiones (salvo las requeridas por las Fuerzas y cuerpos de seguridad del estado), tampoco se realizarán transferencias internacionales. El periodo de retención será de un mes, pudiendo extenderse cuando se solicite siguiendo los procedimientos establecidos en la ley. Pese a que no se basa en el consentimiento, seguirá siendo necesario informar a los afectados de sus derechos mediante un cartel informativo en las instalaciones, pudiendo estos ejercer sus derechos ante el responsable del tratamiento.

Pasemos a abordar ahora los casos particulares que se dan en los distintos negocios ficticios propuestos.

Restaurante S.L realiza una actividad de tratamiento adicional a las ya expuestas, la gestión de reservas. Esta actividad de tratamiento tiene la finalidad de conocer que mesas estarán ocupadas, cuando y quién es el responsable de la reserva. Una novedad de este sistema es que permite conocer si un cliente ha realizado reservas en restaurantes que utilicen el mismo sistema, para evitar conflictos de agenda. También se conservarán los datos para enviar promociones a los clientes. Todo lo relativo a la gestión de la reserva se puede basar en la relación contractual que es la propia reserva. No obstante, es dudoso que la cesión de datos a otros restaurantes pueda sustentarse en esa base o en otra distinta del consentimiento. Además, el envío de comunicaciones promocionales únicamente puede sustentarse en el consentimiento. Los datos tratados serán el nombre, el número de teléfono y la dirección de correo electrónico, todos ellos datos personales identificativos del cliente, ninguno de carácter sensible. El periodo de retención será de un mes desde la reserva salvo que su haya consentido el envío de comunicaciones, en este caso, se retendrán los datos mientras no se retire el consentimiento. El sistema utilizado es una plataforma en la nube que se encuentra hospedada en Estados Unidos, por lo que será necesario informar de la existencia de transferencias internacionales y de la cesión a la empresa en calidad de encargado de tratamiento.

Farmacia S.L realiza un tratamiento cuya finalidad es recomendar nuevos productos a sus clientes, basándose en los productos o servicios que hayan consumido en el pasado. Por ejemplo, un interesado que acude regularmente a la farmacia a tomarse la tensión y obtiene valores ligeramente altos, podría estar interesado en comprar medicamentos para tenerla controlada (estamos suponiendo que no requieren de receta médica). Otro caso, podría ser un interesado que compra cremas antienvejecimiento y estaría interesado en conocer que ha salido al mercado una nueva crema que tiene muy buenos resultados. Claramente, los datos recogidos son datos relativos a la salud de los interesados. Este tipo de actividades de tratamiento de datos únicamente pueden basarse en el consentimiento. Por tanto, el periodo de retención de los datos estará ligado a la existencia del consentimiento no pudiendo extenderse si este es retirado por el interesado. El sistema utilizado por Farmacia S.L para la gestión de la actividad de tratamiento, es un sistema informático instalado en los ordenadores del local, por lo que no se realiza ningún tipo de cesión de datos ni transferencia internacional.

Una de las particularidades de Zapatería S.L es que cuenta con una página web y, aunque la venta online la realiza mediante Amazon, utiliza su web para mostrar información sobre el negocio, incluyendo alguno de sus productos estrella. Además, utiliza Google Analytics para monitorizar el tráfico que recibe la web. Aunque no es estrictamente parte de la normativa de protección de datos, aprovechamos para mencionar que este tipo de páginas web deben cumplir

[24] Informe jurídico, interés legítimo (AEPD). https://www.aepd.es/documento/informe-juridico-rgpd-interes-legitimo.pdf

con la Ley de Servicios de la Sociedad de la Información. Esto implica que deben incluir información de contacto y mercantil sobre el negocio. En cuanto a la actividad de tratamiento aquí realizada, esta tiene la finalidad de conocer el uso que realizan los interesados de su sitio web: que paginas visitan, desde donde acceden, como han llegado al sitio… Este tratamiento se basa en el consentimiento de los interesados. Se recogen datos de navegación del usuario, estos datos están asociados a una cookie y no hay forma de asociarlos al interesado. El periodo de retención de los datos es el periodo máximo de retención que el servicio de Google permita, no están vinculados al consentimiento, ya que no hay una vinculación directa con el interesado. Además, no hay cesión de datos personales ni transferencias internacionales. Esta información se incluirá en la política de cookies. En cuanto a la política de privacidad, siempre es recomendable incluir la parte que afecta a los servicios ofertados en la web, ya que incluir aspectos irrelevantes para el usuario (como la gestión de proveedores), puede saturar de información innecesaria al lector. Sin embargo, en casos como este se podría incluir una política de privacidad que aporte datos básicos (responsable de tratamiento, ejercicio de derechos) e incluya la política de cookies.

Al igual que en el caso anterior, Tintorería S.L cuenta con una web que da publicidad a sus servicios, por tanto, las actividades de tratamiento a definir serán las mismas. No obstante, hay una diferencia fundamental con el caso anterior que merece la pena destacar. La web de Tintorería S.L permite a sus usuarios suscribirse a un boletín informativo para estar al día de las novedades de la limpieza de prendas. En este caso únicamente se recoge el dato personal del correo electrónico o número de teléfono móvil (envío por mensajería instantánea, Whatsapp). Este tratamiento se basa exclusivamente en el consentimiento y los datos personales se retendrán mientras este no se retire. No se realizan transferencias internacionales, pero si se utiliza un servicio de envío para gestionar el boletín, existirá una relación de encargado de tratamiento.

6.1.3 Análisis de riesgos

Tres de los negocios ficticios analizados podrán realizar un análisis de riesgos básico. Sin embargo, Farmacia S.L desea realizar un perfilado de clientes tratando datos sensibles, en concreto, datos relativos a la salud de los interesados. Este tipo de actividades de tratamiento requieren de un análisis de riesgo formal, utilizando una metodología reconocida y una evaluación de impacto. En estos casos se recomienda subcontratar el proceso dada su complejidad. En cuanto al resto de negocios, propondremos ejemplos concretos de datos para los que se realizará una propuesta de amenazas, análisis de riesgos. También se sugerirán medidas de seguridad para mitigar el riesgo.

Analicemos algunas de las amenazas a las que está sometida la actividad de tratamiento de la gestión de reservas de Restaurante S.L. El análisis mostrado a continuación no es exhaustivo, existen más amenazas a las que está sometida la actividad que no han sido tenidas en cuenta en este ejemplo, como la caída del servicio.

Actividad de tratamiento	Amenaza	Impacto	Probabilidad	Riesgo	Medidas para mitigar el riesgo
Gestión de reservas	Acceso no autorizado	Limitado	Improbable	Bajo	Riesgo aceptable, no se aplican medidas
	Incumplimiento de las obligaciones del encargado	Limitado	Baja	Medio	Cláusulas contractuales
	Phishing	Limitado	Media	Medio	Formación de empleados, simulacros de phishing

Tabla 2. Ejemplo de análisis de riesgo. Fuente: Elaboración propia.

En primer lugar, se analizó la amenaza del acceso no autorizado al sistema de gestión de reservas. El impacto que pueda darse en caso de materializarse la amenaza será limitado, ya que los datos que se utilizan en este caso son datos identificativos (nombre, teléfono…). La probabilidad de materialización de la amenaza será improbable. No existen eventos previos de acceso no autorizado a este tipo de sistemas. Además, el sistema de gestión de reservas se encuentra hospedado en un servicio en la nube que cuenta con los más altos estándares de ciberseguridad. Finalmente, el sistema cuenta con configuración de acceso y permisos, lo que permite a Restaurante S.L garantizar que el acceso está controlado. Como resultado del análisis previo se concluye que el riesgo de esta amenaza es bajo y, al tratarse de un nivel de riesgo aceptable, no es necesario implementar medidas de seguridad específicas para mitigarla.

La siguiente amenaza analizada fue el incumplimiento de las obligaciones relativas a la normativa de protección de datos por parte del encargado. Al igual que para la amenaza anterior el impacto es limitado, debido a los datos personales que se verían afectados. En cuanto a la probabilidad, asignamos un nivel bajo. Esto se debe a que la empresa en cuestión no está localizada en ningún estado miembro del Espacio Económico Europeo (es una empresa con sede en Estados Unidos sin presencia física en Europa). Pese a todo, esta empresa se toma muy en serio las normativas de privacidad y asegura un cumplimiento total del Reglamento Europeo de Protección de Datos. El nivel de riesgo resultante del análisis previo es el nivel medio, en este caso será necesario incluir una medida de seguridad para mitigar el riesgo. La medida de seguridad escogida son las cláusulas de encargado de tratamiento. Esta medida, además de ser obligatoria, nos permite establecer una relación contractual para el tratamiento que permita llevar a cabo las acciones pertinentes en caso de incumplimiento, prestando especial atención a las particularidades de la relación internacional.

Finalmente, analizamos la amenaza del phishing. Esta amenaza consiste en la recepción de un correo electrónico fraudulento que incita al receptor a realizar una acción que ponga en peligro los datos del sistema de gestión de reservas. Nuevamente, el impacto es limitado debido al tipo de datos tratados. Sin embargo, hemos asignado una probabilidad media para esta amenaza. En general, el phishing es una técnica muy utilizada para obtener acceso, de manera ilícita, a todo tipo de sistemas. Aunque es cierto que los sistemas de gestión de reservas como este no suelen ser un objetivo tradicional hoy en día, no es descabellado pensar que puedan serlo en un futuro cercano. El nivel de riesgo final es medio, por tanto, es necesario implementar medidas técnicas de seguridad. El método de acción más común para contrarrestar el phishing es la formación. El conocimiento de las técnicas empleadas por los ciberdelincuentes para llevar a cabo estos engaños es la mejor herramienta para identificarlos. Además, existen empresas que organizan simulacros

de phishing. Estos consisten en el envío de correos electrónicos similares a los que enviarían los atacantes con el objetivo de evaluar la respuesta del personal de la empresa.

Tras la realización del análisis de riesgos existen un par de amenazas que deben ser mitigadas. Para ello se procederá a implementar las medidas de seguridad. A continuación, se realiza el análisis de nuevo para comprobar si las medidas son suficientes para alcanzar el nivel de riesgo aceptable.

Actividad de tratamiento	Amenaza	Impacto mitigado	Probabilidad mitigada	Riesgo residual
Gestión de reservas	Acceso no autorizado	Limitado	Improbable	Bajo
	Incumplimiento de las obligaciones del encargado	Limitado	Improbable	Bajo
	Phishing	Limitado	Improbable	Bajo

Tabla 3. Evaluación del riesgo residual tras la aplicación de medidas de seguridad. Fuente: Elaboración propia.

6.1.4 Medidas de seguridad

La gestión de incidentes es uno de los elementos que implica la implementación de medidas de seguridad. Aunque es probable que del análisis de riesgos surja la necesidad de implementar medidas relativas a la gestión de incidentes, es además un requisito de la norma. Por tanto, en este caso práctico nos centraremos en este tipo de medidas. La gestión de incidentes es el proceso que se debe seguir para gestionar una brecha de seguridad, en concreto, la regulación requiere la notificación del incidente a la autoridad de control y a los interesados en ciertos casos. Para poder cumplir con estas obligaciones hay que ser capaz de detectar el incidente y de recopilar la información necesaria para entender que datos han sido afectados. Otro de los elementos fundamentales de la gestión de incidentes es la capacidad de reaccionar a estos y tener la capacidad de volver a la normalidad. Para poder cumplir con todo lo anterior se proponen medidas como: instalación de software antimalware, control de acceso, activación de sistemas de registro ("*logging*") y la realización de copias de seguridad.

La instalación software antimalware es sencilla, simplemente debemos elegir un software que disponga de capacidades de detección y respuesta (EDR). Este tipo de software no solo escanea las firmas de los archivos y las comparan con una base de datos, sino que también monitorizan el comportamiento de los programas para detectar actividades sospechosas.

El control de acceso es una medida que permite limitar el acceso a los sistemas que realizan actividades de tratamiento. Esta medida es un requisito necesario para poder conocer quien tiene acceso a los datos personales y cuando.

Los sistemas de registro permiten almacenar los eventos que ocurren durante el transcurso de las actividades de tratamiento. Estos sistemas almacenan un histórico de los eventos ocurridos, pudiendo consultar en cualquier momento que actividades se llevaron a cabo sobre los datos personales.

Las medidas anteriores nos permiten prevenir, detectar y analizar los incidentes que puedan ocurrir. No obstante, hay un cuarto elemento necesario, la capacidad de recuperación. Pese a la presencia de medidas de prevención, existe la posibilidad de que un incidente se termine materializando. En estos casos, debemos de disponer de una estrategia de vuelta a la normalidad. En prácticamente todos los incidentes, las copias de seguridad son un elemento fundamental de

respuesta. Por ejemplo, uno de los incidentes más frecuentes que afectan simultáneamente a la confidencialidad, integridad y disponibilidad de los datos; son los ataques de "*ransomware*". Estos ataques, además de sustraer información, cifran todos los archivos del sistema imposibilitando el acceso y exigen el pago de un rescate para recuperar la información.

A continuación, vamos a poner un ejemplo de brecha de seguridad de datos personales en Farmacia S.L. Este negocio cuenta con todas las medidas de seguridad descritas anteriormente.

Un empleado de Farmacia S.L está revisando el correo electrónico, muchos de los correos son publicitarios o irrelevantes, la mayoría los podríamos calificar de correo basura. Sin embargo, entre toda la cantidad de correo basura se atisba un mensaje que parece legítimo, es una comunicación del colegio de farmacéuticos al que está adscrito el titular de la farmacia. El correo contiene el asunto «*Recomendaciones para el cumplimiento de la normativa de protección de datos*» y un archivo PDF. Este tipo de comunicaciones no son frecuentes, pero tanto la dirección de correo como el contenido parecen legítimos, por lo que decide abrir el fichero.

El empleado comienza a leer el documento cuyo contenido son recomendaciones reales y basadas en la normativa. Pero, mientras tanto, un programa malicioso cuidadosamente escondido e indetectable por los motores de antivirus, ha comenzado a escanear el sistema en busca de archivos que puedan contener información valiosa. Rápidamente, este programa detecta la base de datos que contiene la información sobre las compras de los clientes miembros del programa de recomendaciones. Tras lo cual comienza la exfiltración de datos y, simultáneamente, el cifrado de la base de datos. Por suerte, el sistema cuenta con un software de detección y respuesta (EDR) de última generación. Tras detectar esta actividad sospechosa, cifrado y envío de grandes volúmenes de información fuera de la red, el sistema decide aislar el proceso y notificar al usuario. Además, durante todo este tiempo un sensor de registro de actividad ha estado enviando los eventos que se sucedían a un sistema externo de almacenamiento y gestión de eventos automatizado (SIEM). Este sistema ha detectado que el dispositivo ha realizado una serie de acciones sospechosas y, junto con la alerta del sistema EDR, ha emitido una notificación a la empresa externa de ciberseguridad encargada de monitorizar los sistemas de registro.

Llegados a este punto, podemos constatar que se ha producido una brecha de seguridad en los sistemas de Farmacia S.L. Por suerte, las medidas de seguridad proactivas han funcionado y se ha detenido el ataque, en este momento comienza el proceso de gestión de incidentes. El sistema informático de Farmacia S.L está completamente inutilizado por lo que es necesario bajar la persiana hasta que el problema se solucione. Ahora es necesario comprender que ha ocurrido e iniciar el proceso de vuelta a la normalidad tan pronto como sea posible. Gracias al sistema de gestión de eventos, la empresa externa de ciberseguridad ha podido determinar el origen del software malicioso, una vez constatado que el origen es realmente el colegio de farmacéuticos, se ponen en contacto con ellos para que hagan todo lo necesario para evitar la propagación del software malicioso a otras farmacias. Continuando con la investigación, se descubre que el "*malware*" ha accedido a la base de datos de recomendaciones, que contiene datos de carácter sensible de los interesados, por desgracia el servidor local de copias de seguridad también ha sido comprometido. La investigación también permite descubrir que hubo múltiples intentos de acceso al sistema de receta electrónica. No obstante, el robusto sistema de control de acceso y una estricta política de contraseñas evitaron que se propagara a ese sistema.

Finalizada la investigación, se dispone de una cronología de eventos en el sistema SIEM, así como de evidencias sobre el origen de la amenaza. Un correo malicioso procedente de un tercero de confianza desencadenó una brecha de seguridad que fue detenida antes de que se completaran la exfiltración y el cifrado de datos. El sistema de control de accesos evitó la propagación al sistema de receta electrónica, pero no impidió que se corrompiera la copia de seguridad local. Por suerte, Farmacia S.L había implementado un sistema de copia de seguridad teniendo estas situaciones en cuenta, siguiendo la regla 3, 2, 1 (tres copias de los datos, al menos dos soportes distintos y un sistema externo). La estrategia de copia de seguridad seguida ha permitido que

exista una copia que no se ha visto comprometida en el ataque, la copia externa. Estas copias se realizan diariamente, por lo que se ha producido una pérdida irrecuperable de los datos más recientes, debido a que la farmacia ya llevaba unas horas abierta. Además, restaurar copias de seguridad desde un sistema externo es un proceso lento que puede durar varias horas. Pese a lo anterior, esta copia de seguridad nos permite iniciar el proceso de vuelta a la normalidad. Lo que permitirá a Farmacia S.L recuperar la práctica totalidad de los datos y levantar la persiana solo un día después desde que se produjo el incidente de seguridad.

Hasta ahora nos hemos centrado en el proceso técnico de la gestión del incidente. Pero para cumplir con la normativa de protección de datos puede ser necesario notificar a la autoridad de control y a los interesados. Atendiendo a los criterios estipulados por la ley para determinar los casos en los que es necesario llevar a cabo una notificación, podemos concluir que este es uno de ellos. Esto se debe a que se han visto afectados datos sensibles que pueden suponer un alto riesgo para las libertades y los derechos fundamentales de los interesados. Dado que se ha determinado la necesidad de notificar, disponemos de 72 horas desde que tenemos conocimiento del incidente para proporcionar toda la información necesaria relativa al incidente a la autoridad de control. Además, pese a que la base de datos está cifrada cuando no se usa, es altamente probable que, dado que el sistema estaba activo cuando se produjo el incidente, se hayan producido filtraciones de datos sensibles de los interesados. En estos casos, también será necesario el envío de una notificación a los afectados. Pese a que el ataque se detuvo rápidamente y es muy probable que la filtración solo afecte a un número reducido de interesados, no ha sido posible identificar quienes son los afectados. Por tanto, se ha decidido enviar una notificación a todos los interesados que otorgaron su consentimiento para participar en el programa de recomendación. Finalmente, se decide denunciar lo ocurrido ante la policía, esto último no es un requisito de la normativa de protección de datos pero, al fin y al cabo, los hechos ocurridos son constitutivos de delito.

6.1.5 Gestión del consentimiento

La mayoría de los casos de gestión del consentimiento son sencillo. Básicamente bastará con confeccionar un formulario de recogida de datos (en papel o digital) que incluya los textos legales necesarios para informar al interesado de: sus derechos; todo lo relativo a la actividad de tratamiento, finalidad, base legal, etc. y una casilla para que proporcione el consentimiento de forma explícita. No obstante, habrá casos como los que analizaremos a continuación que cuentan con particularidades que se alejan de este proceso básico.

El sistema de reservas de Restaurante S.L está completamente integrado en su página web. Por tanto, cuando se hace una reserva se presenta un formulario web que, además de los datos de la reserva, recoge el consentimiento de los usuarios. Sin embargo, el restaurante también admite reservas telefónicas y presenciales. En estos casos, quien introduce los datos en el sistema de gestión, es el empleado que toma nota de los datos del cliente. Esta forma de proceder es una clara violación de la normativa. No solo no se está informando al cliente de sus derechos, sino que queda a disposición de quien introduce los datos en el sistema la decisión de marcar la casilla del consentimiento. Para evitar este tipo de situaciones se podría introducir una locución telefónica que informe al interesado de sus derechos, además se deberá solicitar el consentimiento mediante una acción afirmativa, que podría ser grabada como evidencia. En caso de que la reserva se realice en persona sería recomendable contar con un formulario en papel. Otra solución a este problema sería informar al personal de que no debe marcar la casilla de consentimiento. En ese caso, solo se podrán realizar los tratamientos que no se basen en el consentimiento de los interesados. Pero, independientemente de la solución escogida, es necesario informar del tratamiento que se hará con los datos, así como de los derechos que pueden ser ejercidos.

Otra situación que afecta a Restaurante S.L es el reciente cambio en la propiedad. Este cambio afecta directamente a la titularidad del negocio y, por tanto, al responsable del tratamiento. En este caso particular el responsable de tratamiento continúa siendo Restaurante S.L por lo que

no se ha producido ningún cambio relevante que haya que notificar al interesado. Sin embargo, si se tratara de una fusión, absorción o cualquier otro cambio que modifique alguno de los aspectos de las actividades de tratamiento (el cambio de responsable de tratamiento en estos casos) se deberá informar a los interesados inmediatamente, pudiendo estos ejercer sus derechos si así lo desean.

Generalmente, la retirada del consentimiento suele llevar asociada la suspensión del tratamiento y la posterior eliminación de los datos. No obstante, el caso del uso de cookies como la de Google Analytics es diferente. Cuando se otorga el consentimiento para monitorizar la actividad de navegación del usuario en una web, se instala una cookie que se utiliza como identificador de las acciones realizadas. Sin embargo, esta cookie es un identificador anónimo que solo vincula al usuario mientras esta exista en el navegador. Tras la eliminación de la cookie todos los datos recogidos se convierten en estadísticas anónimas e imposibles de trazar. Por tanto, en este caso la retirada del consentimiento solo producirá la eliminación de la cookie y no el borrado de la estadística asociada a los datos de navegación recogidos.

En la exposición de las empresas ficticias se estableció la vinculación entre Zapatería S.L y Tintorería S.L (ambas forman parte de Grupo S.A). Previendo esta situación, Zapatería S.L comenzó a incluir la recogida de datos con fines promocionales incluyendo la cesión de datos a otras empresas de Grupo S.A. Sin embargo, existen consentimientos previos que no contemplan la cesión de datos a otras empresas, aunque si se recogieron con finalidades promocionales. Ahora los dueños de Grupo S.A se preguntan si ese consentimiento se podría utilizar para el envío de campañas promocionales de Tintorería S.L. En general, la respuesta es no. No existe una base legitimadora que pueda sustentar esta acción. Aunque la finalidad es la misma, el consentimiento inicial se otorgó sin mención alguna a la cesión de datos. Si se desea realizar este cambio se deberá recabar el consentimiento de los interesados. No obstante, pueden existir otros casos en los que esta cesión si sea legítima. Por ejemplo, la gestión de clientes (facturación) será realizada por el grupo en vez de por Zapatería S.L. En este caso, se cederán datos personales al grupo sin consentimiento explicito. Esto es posible porque la base legitimadora no es el consentimiento si no la obligación legal.

6.1.6 Ejercicio de derechos

La casuística del ejercicio de derechos es muy amplia, por tanto, es difícil establecer ejemplos que incluyan todos los escenarios posibles. Sin embargo, en este apartado proporcionaremos una serie de ejemplos que ilustren algunos escenarios relevantes.

Supongamos que un interesado solicita ejercer su derecho de acceso a imágenes de videovigilancia. Para atender este tipo de solicitudes puede ser necesario proporcionar las imágenes grabadas. Sin embargo, este tipo de solicitudes pueden ser complejas de atender. No siempre será posible proporcionar una imagen exclusiva del interesado, es posible que haya más personas en la grabación. No obstante, esto no puede ser una excusa para no proporcionar las imágenes. Según la guía de gestión de imágenes de videovigilancia[25] del Comité Europeo de Protección de Datos, se podrá editar el video para proteger la identidad de otros interesados. Otro posible impedimento será la imposibilidad de realizar búsquedas en las grabaciones, hecho que puede dificultar enormemente la tarea de atender la solicitud. En definitiva, atender este tipo de solicitudes es complejo por lo que, si se dan estas circunstancias habrá que analizar cuidadosamente si es justificable denegar la solicitud o si debe atenderse.

Otro caso interesante que puede darse es el ejercicio de un derecho que, por el tipo de datos tratados, no procede. Puede suceder, entre otros, con el derecho de oposición. El derecho de

[25] Guía de videovigilancia Comité Europeo de Protección de Datos https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

oposición podrá ejercerse si el tratamiento de los datos se basa en el interés público o el interés legítimo, también podrá ejercerse para oponerse a la elaboración de perfiles. En caso de que un interesado realice una solicitud de oposición, pero no sé de alguna de las circunstancias anteriores, esta deberá ser denegada.

Uno de los derechos que más ejercidos probablemente sea el derecho de supresión (incluyendo la retirada del consentimiento). Usaremos como ejemplo a Restaurante S.L. Supondremos que el interesado otorgó el consentimiento durante la realización de una reserva. Sin embargo, tras recibir un par de comunicaciones comerciales ha decidido que ya no desea seguir recibiéndolas. En consecuencia, ha decidido ejercitar su derecho de supresión, retirando el consentimiento y solicitando la eliminación de sus datos. En este caso deberemos atender la solicitud mediante el proceso definido en nuestro sistema de gestión, se accederá al sistema de gestión de reservas y se retirará el consentimiento para el envío de notificaciones comerciales. Acto seguido, se comprobará si existe algún motivo para no eliminar los datos, por ejemplo, una disputa judicial. Salvo que exista algún motivo que justifique la retención de los datos del interesado se procederá a la eliminación de estos. Finalmente, se notificará al interesado que su solicitud ha sido atendida, todo esto en un plazo inferior a un mes desde la recepción de la solicitud.

6.1.7 Encargados de tratamiento

En la mayoría de las situaciones, el establecimiento de contratos de encargado de tratamiento por parte del pequeño comercio dará lugar a contratos que son propuestos por una entidad más grande y con mayor poder de negociación. Siempre deberemos comprobar que dichos contratos cumplen con los requisitos mínimos y hacer todo lo posible para añadir aquellas cláusulas que, siendo necesarias, no hayan sido ya incluidas. En este apartado no describiremos todas las situaciones posibles, solo aquellas para las que concurra algún aspecto relevante que merezca la pena analizar. Sin embargo, será necesario establecer un contrato de encargado en todas aquellas situaciones para las que se haya detectado que existe dicha relación.

Farmacia S.L cede datos de facturas a una gestoría, se debe evitar proporcionar el detalle de la factura, ya que contiene datos sensibles y es innecesario para las tareas de la gestoría. Esto simplificará mucho el contrato de encargado de tratamiento, ya que las medidas de seguridad exigidas podrán ser menos exigentes. Es bastante probable que la gestoría utilice un modelo de contrato propio para el establecimiento de la relación de encargado de tratamiento. No obstante, deberíamos de comprobar que las cláusulas se ajustan a los requisitos mínimos establecidos en el procedimiento y proponer subsanar las deficiencias (de haberlas) utilizando alguna de las cláusulas tipo propuestas por la Comisión Europea.

Tintorería S.L cuenta con una página web que, además de proporcionar información sobre los servicios que ofrece, permite suscribirse voluntariamente a comunicaciones comerciales. Toda la gestión de las comunicaciones comerciales se realiza en el propio servicio de hospedaje. Podríamos pensar que, dado que el tratamiento de los datos lo realiza íntegramente el responsable, no es necesario establecer un contrato de encargado ya que no hay acceso a los datos. Sin embargo, el servicio de hospedaje es un encargado de tratamiento sin acceso a los datos. Al estar en posesión de datos personales deberá implementar las medidas de seguridad necesarias para evitar el acceso no autorizado a los datos, así como comprometerse a la confidencialidad de aquellos datos a los que haya podido tener acceso de forma accidental. Nuestro contrato de tratamiento deberá excluir todos aquellos aspectos que no encajen en esta forma de relación. Por ejemplo, no tendrá sentido derivar al encargado el ejercicio de derechos de los interesados o forzar al encargado a mantener un registro de las actividades de tratamiento de la actividad comercial.

Restaurante S.L cede datos al sistema de gestión de reservas. Esta es una relación de encargado de tratamiento del mismo tipo que la del ejemplo de Tintorería S.L, es decir, una relación de encargado sin acceso a datos. No obstante, en este caso hay que incluir las

particularidades de la transferencia internacional. Para el caso que nos ocupa la transferencia internacional se realiza a un país fuera del Espacio Económico Europeo. En estos casos, será necesario comprobar si la Comisión Europea ha emitido una decisión de adecuación, como si ha hecho para Estados Unidos. Al existir una decisión de adecuación es más que suficiente con el establecimiento de un contrato con las mismas cláusulas que tendría uno a nivel nacional. De no existir esa decisión sería necesario realizar un proceso más complejo. No detallaremos los pormenores de este proceso aquí, aunque se puede consultar el material de apoyo de la Agencia Española de Protección de Datos[26].

Zapatería S.L es vendedor en Amazon, pero gestiona sus propios envíos. En estos casos Amazon habrá establecido un contrato de encargado de tratamiento con Zapatería S.L. Será muy importante verificar que este contrato permite subcontratar partes del tratamiento de datos, de lo contrario, no se podría subcontratar la entrega con un servicio de mensajería. En estos casos, aunque no seamos el responsable de tratamiento, deberemos establecer un contrato de encargado de tratamiento con el servicio de mensajería y trasladar todas las cláusulas que Amazon establezca para este tipo de contratos.

6.1.8 Delegado de protección de datos

De los casos prácticos propuestos solo Farmacia S.L cumple con alguno de los criterios que hacen obligatorio el DPD. Por tanto, utilizamos dicho negocio como ejemplo del análisis a realizar. Las farmacias tratan datos relativos a la salud y el artículo 37.1.c establece que si este tratamiento es a gran escala es obligatorio contar con DPD, por tanto, dependerá de si este criterio aplica o no. Para aportar claridad podemos utilizar el criterio de la AEPD[27] para determinar que, en general, una farmacia no está obligada a contar con un DPD. No obstante, nuestro caso práctico a establecido que el negocio va a realizar actividades comerciales basadas en el perfilado de los interesados. Es decir, en base a sus compras se elaborará un perfil del interesado para realizar recomendaciones. Esta actividad de tratamiento se encuentra definida en el artículo 34.1.k de la LOPDGDD (9). Por tanto, para nuestro caso práctico si es necesario contar con DPD. Dado que la presencia del DPD en este negocio es requerido, se decide subcontratar este rol con una empresa externa. Para esta contratación se priorizarán aquellos que puedan aportar un certificado de DPD y, en caso de no ser posible, se aplicarán los criterios establecidos en el procedimiento.

[26] Garantías de transferencia de datos personales AEPD. https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-transferencias-datos-personales

[27] FAQ sobre el delegado de protección de datos (AEPD). https://www.aepd.es/preguntas-frecuentes/4-dpd/1-delegado-de-proteccion-de-datos/FAQ-0403-que-significan-actividad-principal-observacion-sistematica-tratamiento-gran-escala

7 Pruebas

Este sistema de gestión se ha abordado de manera teórica, por lo que su utilidad final queda pendiente de validar en términos prácticos. Sin embargo, en este trabajo proponemos seguir el mismo proceso que se lleva a cabo con cualquier sistema de gestión. Los sistemas de gestión proponen una metodología denominada PDCA (en inglés, "*Plan*", "*Do*", "*Check*", "*Act*"). Esta metodología en cuatro fases busca establecer un proceso iterativo de mejora. Este ciclo se repite una y otra vez con el objetivo de que, tras cada iteración, el sistema se transforma adaptándose a las necesidades del negocio y a los cambios normativos. Tras cada iteración, el sistema se vuelve más correcto (adaptado a la normativa) y más eficiente (adaptado a los procesos del negocio). Este proceso es el que se siguió durante la implantación inicial. La fase de planificación ("*Plan*") es la propia metodología de implantación. La siguiente fase, la implementación ("Do"), consiste en seguir, paso a paso, el plan establecido por la metodología de implantación. A continuación, la fase de comprobación ("*Check*") se centra en revisar la implantación para comprobar que se cumple la normativa y que el sistema se adapta correctamente a los procesos de la organización. Esta fase se corresponde con el último punto propuesto en nuestra metodología de implantación, las auditorías. Finalmente, para completar el proceso iterativo, es necesario llevar a cabo un proceso de corrección ("*Act*") de las deficiencias halladas. Este proceso final de corrección se desarrolla implementando planes de acciones correctivas. Estos planes son el resultado del proceso anterior y un elemento a tener en cuenta en la siguiente iteración. Un plan de acción correctiva (PAC) comienza enumerando las deficiencias halladas en la fase de comprobación. Acto seguido, deberemos analizar cuál es el origen de esas deficiencias y cuáles fueron las causas que las hicieron posible. De esa forma, el plan que desarrollemos para corregirlas podrá incluir acciones para evitar que se vuelvan a producir. Finalmente, se procederá a la implementación de las acciones correctivas, lo que marca el inicio de una nueva iteración.

A continuación, pasamos a centrarnos en la fase de comprobación. Como ya se ha comentado anteriormente, existen dos opciones para verificar la validez de nuestro sistema: la auditoría interna y la auditoría externa. Aunque hay dos opciones, estas no son excluyentes. En nuestra metodología de implantación propusimos llevar a cabo una auditoría interna como requisito indispensable, mientras que la auditoría externa sería completamente opcional (aunque recomendable). En este apartado nos centramos en la auditoría interna y en cómo llevarla a cabo.

Una auditoría interna no es más que una revisión punto por punto del estado de cumplimiento de cada uno de los aspectos relevantes de la normativa. Para llevar a cabo este proceso introducimos dos herramientas fundamentales: la declaración de aplicabilidad y el modelo de madurez de las capacidades CMM (siglas en ingles de "*Capability Maturity Model*").

- Modelo de madurez de las capacidades: este modelo permite evaluar de forma cualitativa el grado de madurez de un proceso concreto. Esta evaluación nos permitirá establecer, junto con la declaración de aplicabilidad, una métrica única que permitirá conocer rápidamente el estado global del sistema de gestión. Este modelo de madurez de procesos establece seis niveles:

    - L0 Inexistente: no existe ningún proceso definido para el cumplimiento de la medida. Este nivel, el más bajo, es aquel en el que se encontrarán la mayoría de los procesos (sino todos) antes de la implantación del sistema.

    - L1 Inicial: existen procesos para el cumplimiento de las medidas. No obstante, estos procesos no están formalizados, se aprenden con la práctica y cada miembro del equipo que lo realiza puede introducir variaciones dada la ambigüedad existente en cada proceso. En nuestro

sistema de gestión no debería existir ningún proceso de este tipo ya que se han definido procedimientos para cada uno de los aspectos fundamentales. Es bastante probable que existan procesos que puedan clasificarse con este nivel de madurez antes de la implantación.

- L2 Repetible: existen procesos para el cumplimiento de las medidas. Sin embargo, al igual que para el nivel anterior, no existen procesos formales definidos, los procesos se trasmiten con la experiencia. La principal diferencia de este nivel es que, por el motivo que sea, los encargados de realizarlo han alcanzado un grado de experiencia práctico que les permite desarrollar el proceso de manera sistemática, repitiendo siempre los mismos independientemente de quién sea el encargado de realizar las tareas. Al igual que en los niveles anteriores, se espera que existan procesos con este nivel de madurez antes de la implantación del sistema de gestión.

- L3 Definido: existen procesos documentados mediante procedimientos. La existencia de procedimientos documentados que definen los procesos permite que ninguna de las tareas asociadas quede al azar. Además, las tareas puedan ser realizadas por cualquier miembro del equipo, independientemente de su formación y experiencia. Este nivel de madurez es el mínimo necesario para poder cumplir con la normativa de protección de datos. Además, es el nivel que se espera alcanzar con la implantación del sistema.

- L4 Gestionado: existen procesos documentados y medibles. Este nivel de madurez incorpora a los procesos definidos métricas sobre su eficiencia y calidad. Estas métricas de carácter cuantitativo permitirán evaluar el estado de los procesos mediante técnicas estadísticas. No es objetivo de nuestro sistema de gestión alcanzar este estado, aunque con el tiempo, se pueden mejorar los procesos establecidos para incorporar métricas.

- L5 Optimizado: existen procesos documentados, medibles y esos se mejoran proactivamente. Este nivel de madurez, el más alto, incorpora los anteriores y añade un componente de mejor proactiva. Las métricas definidas se utilizan para detectar aspectos de mejora y para establecer objetivos que deben alcanzarse. Cualquier desviación de los objetivos se traduce en acciones a realizar para alcanzarlos de nuevo. Al igual que con el nivel cuatro, no es objetivo del sistema desarrollado alcanzar este grado de madurez. No obstante, si se decide progresar al cuarto nivel de madurez debería ser posible llegar a alcanzar el máximo.

- Declaración de aplicabilidad: una declaración de aplicabilidad es un documento que detalla, punto por punto, todas las medidas que es posible implementar para alcanzar el cumplimiento de una norma. Este documento, permite establecer qué medidas se han implementado, cuáles no y por qué (por ejemplo, si no contamos con delegado de protección de datos, justificaremos por qué no es necesario). Además, este documento puede utilizarse como guía para enlazar a los procedimientos y registros que evidencian el cumplimiento de las medidas implementadas. Para elaborar este documento se han utilizado (25, 36).

Finalmente, hemos definido una métrica que utiliza la declaración de aplicabilidad y el nivel de madurez de cada control para calcular un índice de cumplimiento. Este índice, en forma de porcentaje, alcanzará el 100% si todas las medidas implementadas alcanzan un grado de madurez L3.

Control	Nivel de madurez	¿Requerido?	¿Por qué no es requerido?	Implementado	Detalles de implementación
Condiciones para la recolección y procesamiento					
Identificar y documentar la finalidad	0	Si		No	
Identificar la base legitimadora	0	Si		No	
Determinar cómo y cuándo se obtiene el consentimiento	0	Si		No	
Obtención y registro del consentimiento	0	Si		No	
Evaluación de impacto	0	No		No	
Contratos de encargado del tratamiento	0	Si		No	
Registro de actividades de tratamiento	0	Si		No	

Tabla 4. Extracto de la declaración de aplicabilidad. Fuente: Elaboración propia.

Como podemos ver en la Tabla 4 cada uno de los controles cuenta con los parámetros necesarios para determinar si un control es requerido y su estado de implementación. Finalmente, la tabla incluye una columna para determinar el nivel de madurez. Este nivel se utilizará para el cálculo del índice de cumplimiento descrito anteriormente.

8 Conclusiones

Al comienzo de este trabajo, nos emplazamos a diseñar un sistema de gestión de la privacidad adaptado al pequeño comercio con el fin garantizar el cumplimiento de la normativa en vigor en materia de protección de datos. Además, también se propuso establecer dos elementos fundamentales. La creación de ejemplos de aplicación (casos prácticos) y el diseño de una metodología de validación del sistema creado. Llegados a este punto, podemos decir que los objetivos propuestos han sido alcanzados con éxito. No obstante, merece la pena realizar una revisión de lo conseguido y de lo aprendido para sentar las bases de futuras aportaciones al ámbito abordado.

Durante el desarrollo del sistema de gestión se ha profundizado en los aspectos legales de estas regulaciones. En concreto, ha sido necesario acudir directamente a los textos legales del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales (LOPDGDD). Además, esta legislación crea organismos supervisores; por lo que también se acudió a sus respectivos portales para acceder a las decisiones emitidas, las guías creadas y las normas desarrolladas como parte de su función supervisora. Esta amplia base de material normativo fue el germen de la motivación original para la realización de este trabajo. Es decir, simplificar las tareas necesarias para alcanzar el cumplimiento de la normativa en el pequeño comercio. Este tipo de negocios no cuenta con amplios recursos económicos que les permitan "comprar" una solución personalizada, por lo que muchas veces se pueden encontrar situaciones de cumplimiento parcial o de incumplimiento manifiesto. No obstante, sería incorrecto concluir que nuestro sistema de gestión es una solución completa. Existen multitud de casos para los que no ha sido posible incluir ejemplos, dada la enorme casuística que puede darse. Este es, sin duda, uno de los aspectos que nos hacen concluir que aún quedan aspectos por desarrollar.

Desde el principio hubo aspectos que se excluyeron dada su complejidad. Un claro ejemplo de esto es la evaluación de impacto. Este proceso es complicado y en un principio se decidió que su inclusión quedaría reducida al mero reconocimiento de su existencia. Sin embargo, durante el desarrollo del trabajo, se decidió incluir un desarrollo algo más profundo ya que es un aspecto que debe estar incluido en el sistema de una forma u otra. La solución para la inclusión de este aspecto fue una contribución parcial. La evaluación de impacto sigue siendo un aspecto complejo, pero proponemos un método de determinación de su necesidad y, en caso afirmativo, la externalización del proceso. Por el contrario, la inclusión de otro aspecto relevante, el ejercicio de derechos de los interesados fue tenida en cuenta desde el principio. Nuestro sistema proporciona una metodología consistente que permite atender la mayoría de las solicitudes. No obstante, existen casos particulares no triviales que pueden requerir de asistencia legal, por lo que nuestra solución dista de ser perfecta.

Uno de los efectos secundarios del estudio de la regulación y de cómo aplicarla en el mundo real, es que nos ha permitido interiorizar la dificultad a la hora de proteger los derechos de los ciudadanos sin provocar efectos indeseables, como el perjuicio a la actividad económica. La lectura de la legislación permite apreciar la introducción de cierta ambigüedad y puntos de extensión que, interpretamos, tienen el objetivo de incluir las múltiples situaciones que existen dentro del ámbito de aplicación de la normativa. Sin embargo, este tipo de tácticas pueden ser un arma de doble filo, ya que permiten a instituciones no electas establecer restricciones que pueden resultar en efectos de segunda ronda no previstos. Es un hecho que existe una tensión entre estos dos aspectos que debe tenerse en cuenta en el desarrollo de cualquier legislación y que la dificultad de este problema aumenta a medida que se amplía su ámbito de aplicación.

Hasta ahora las autoridades de control han utilizado estos puntos de extensión para proporcionar guías aclaratorias, formación, clausulas tipo… Estos elementos de ayuda son fundamentales para aportar claridad y certidumbre sobre los aspectos más ambiguos de la norma,

aunque no siempre están disponibles cuando los necesitamos. Por ejemplo, el dictamen de la Comisión Europea sobre las cláusulas tipo para los contratos de encargado de tratamiento se publicó en 2021, mientras que la legislación fue aprobada en 2016 y entró en vigor en 2018. Es cierto que algunas autoridades de control ya habían publicado las suyas propias,y que es necesaria una revisión previa por parte del Comité Europeo de Protección de Datos. No obstante, en nuestra opinión, los retrasos en la elaboración de este tipo de elementos suponen una carga añadida para aquellos negocios que no cuentan con amplios recursos económicos. Otro ejemplo de esto último es la ausencia de un esquema de certificación en materia de protección de datos. Aunque podemos esperar que esto se solucione "pronto", ya que así se propone en el eje 4.6 del Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos (37).

Por otro lado, existen puntos de extensión que dependen directamente de los propios negocios y que pueden ayudar a simplificar la implantación de la legislación. Estamos hablando de los códigos de conducta. La adhesión a un código de conducta puede simplificar enormemente la implantación de la normativa. Los códigos pueden ser desarrollados por empresas, asociaciones, colegios profesionales… y registrados ante la AEPD. Además, estas entidades cuentan con mayores recursos y poseen mayores conocimientos sobre los negocios que más dificultades tienen a la hora de adecuarse a la normativa. Creemos que de existir estos códigos se reducirían significativamente los costes y el tiempo de adecuación, así como la incertidumbre provocada por la ambigüedad de algunos aspectos de la regulación. Por esto último, celebramos que el eje 4.7 del plan estratégico de la AEPD (37) consista en incrementar la colaboración con asociaciones empresariales y colegios profesionales. Quizá este punto sea el impulso que se necesita para el desarrollo de este aspecto.

A pesar de los contratiempos y limitaciones mencionadas en los párrafos anteriores creemos que la introducción de este sistema viene a rellenar una de las mayores deficiencias detectadas, la falta de énfasis en los procesos de auditoría e inspección. Gracias al sistema desarrollado, se permite incorporar de manera orgánica las evidencias necesarias para demostrar el cumplimiento ante agentes externos como la autoridad de control, la Agencia Española de protección de datos. Este elemento es fundamental para evitar sanciones, ya que permite demostrar el cumplimiento. Esperamos que este sistema siente las bases de otros más completos en el futuro y que permita finalmente alcanzar la visión expuesta en el Considerando segundo del Reglamento General de Protección de Datos:

«…contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.»

8.1 Relación del trabajo desarrollado con los estudios cursados

Este trabajo se ha desarrollado para la asignatura "Trabajo de Fin de Grado" del grado en Ingeniería Informática de la Universidad Politécnica de Valencia. Además de ser un elemento necesario para la obtención del título universitario de grado, es un proyecto que nos ha permitido poner en práctica los conocimientos adquiridos y las competencias transversales desarrolladas.

El grado incluye asignaturas como Fundamentos de organización de empresas que nos enseña cómo se desarrolla un negocio y la importancia del contexto de la organización, en particular, cómo los riesgos regulatorios son una parte fundamental. No es posible llevar a cabo la misión de la organización sin tener en cuenta los aspectos legales que influyen en su desarrollo. Profundizando en el aspecto del cumplimiento legal, encontramos asignaturas como Deontología y profesionalismo. Esta asignatura nos enseña el papel que juegan las leyes en el desarrollo de la profesión del ingeniero informático y, en particular, desarrolla los aspectos fundamentales de las algunas de las que han sido el objeto principal de este trabajo. También, podemos encontrar asignaturas como Gestión de proyectos. Esta asignatura está presente en todo proyecto, de principio a fin. Nos enseña como definir el alcance y demás aspectos fundamentales a desarrollar

(al margen del propio proyecto). Entre estos, podemos encontrar algunos que han sido fundamentales en el desarrollo de este proyecto, por ejemplo, la estimación temporal de las tareas. Finalmente, el grado nos ha aportado los conocimientos necesarios para comprender los aspectos técnicos de las medidas de seguridad. Asignaturas como Redes de computadores nos han permitido comprender los requisitos técnicos de la seguridad de la información en tránsito. Mientras que, asignaturas como Fundamentos de sistemas operativos y arquitectura e ingeniería de computadores, nos han ayudado comprender las estrategias utilizadas por todo tipo de software malicioso para adueñarse de los sistemas informáticos y poner en peligro la seguridad de los datos personales.

Por otro lado, la formación adquirida no es solo de índole técnica, si no que incluye competencias transversales fundamentales para el desarrollo de un trabajo como este. Este trabajo ha requerido del análisis y resolución de problemas para el desarrollo de la solución presentada. En concreto, ha sido necesario desarrollar modelos y procesos abstractos para resolver problemas complejos y poder aplicarlos de manera práctica para resolver problemas reales. También se ha hecho uso de la competencia de aprendizaje permanente. Una gran cantidad del contenido incluido en este trabajo ha requerido del aprendizaje de aspectos sobre la normativa de protección de datos que no se incluyen en el currículo de las asignaturas del grado.

9 Bibliografía

1. WARREN, Samuel D. and BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*. 15 December 1890. Vol. 4, no. 5.

2. NISA ÁVILA, Javier Antonio. *Inteligencia Artificial, IOT, y Data Mining: Una nueva perspectiva jurídica de la Teoría del Mosaico*. Online. 2021. [Accessed 30 November 2024]. Available from: https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

3. *Constitución Española*. 29 December 1978. España.

4. *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.* 14 December 1999. España.

5. *Carta de los derechos fundamentales de la Unión Europea*. 18 December 2000.

6. *VERSIÓN CONSOLIDADA DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA*. 26 October 2012. Unión Europea.

7. *DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO*. 23 November 1995. Unión Europea.

8. *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO*. 27 April 2016. European Union.

9. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. 6 December 2018. España.

10. FREITAS, Maria da Conceição and MIRA DA SILVA, Miguel. GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*. 10 November 2018. Vol. 3, no. 4. DOI 10.20897/jisem/3941.

11. HÄRTING, Ralf Christian, KAIM, Raphael, KLAMM, Nicole and KRONEBERG, Julian. Impacts of the New General Data Protection Regulation for Small- and Medium-Sized Enterprises. In : *Advances in Intelligent Systems and Computing*. Springer Science and Business Media Deutschland GmbH, 2021. p. 238–246. ISBN 9789811558559. DOI 10.1007/978-981-15-5856-6_23.

12. TRAVIESO MORALES, Victoriano, HOUSER, Kimberly A and BARCELONA, JD. *The GDPR Implementation Challenges Faced By Technology Startups In Catalonia DBA Thesis Geneva Business School Doctorate in International Management*. 2023. Date: 30/03/2023 Word count: 43.925

13. *RECOMENDACIÓN DE LA COMISIÓN de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas*. 6 May 2003. Unión Europea : European Comission.

14. *Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista.* 15 January 1996. Españas.

15. LALIGA MÁÑEZ, Zintia Mª. *Adaptación de una pyme a la normativa del RGPD*. . Valencia : Universidad Politecnica de Valencia, 2019.

16. BRODIN, Martin. A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research*. October 2019. Vol. 4, no. 2, p. 243–264. DOI 10.1007/s41125-019-00042-z.

17. EJARQUE, Sahuquillo. *Guía para el cumplimiento normativo en una pequeña organización de la protección de las bases de datos*. . Valencia : Universidad Politecnica de

Valencia, 2024. Guía para el cumplimiento normativo en una pequeña organización de la protección de las bases de datos.

18. MOMPÓ ALBEROLA, Josep. *Guía interactiva para el cumplimiento de las normas de protección de datos en el entorno laboral*. . Valencia : Universidad Politecnica de Valencia, 2020.

19. CHATZIPOULIDIS, Aristeidis, TSIAKIS, Theodosios and KARGIDIS, Theodoros. A readiness assessment tool for GDPR compliance certification. *Computer fraud & security*. August 2019. Vol. 2019, no. 8, p. 14–19. The General Data Protection Regulation (GDPR) is new legislation that governs users' private data and applies across all member states of the European Union (EU), particularly to all organisations processing the data of EU users, wherever the organisation is geographically based. It came into force on 25 May 2018.

20. *Guidelines for SMEs on the security of personal data processing*. ENISA, 2016.

21. AEPD, APDCAT and DATUAK BABESTEKO. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*. 2017.

22. *Practice guide GDPR - Security of personal data 2024* Online. 2024. Available from: www.cnil.fr

23. LLOPIS FERRIOL, Jesús. *Creación de una guía para la aplicación del nivel básico, medio y alto del Reglamento de Protección de Datos para microempresas*. . Valencia : Universidad Politecnica de Valencia, 2016.

24. PEDROSO, Luis M., ARAUJO, Virginia M., COTA, Manuel Perez and MAGALHAES, Joao Paulo. How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data. In : *Iberian Conference on Information Systems and Technologies, CISTI*. IEEE Computer Society, 23 June 2021. ISBN 9789895465910. DOI 10.23919/CISTI52073.2021.9476620.

25. *Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019)*. 2021.

26. *Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. Modificación 1: Acciones relativas al cambio climático. (ISO/IEC 27001:2022/Amd 1:2024)*. 2025.

27. CNIL. Record of processing activities. Online. 20 August 2019. [Accessed 16 August 2025]. Available from: https://www.cnil.fr/en/gdpr-toolkit/record-processing-activities

28. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. 2021.

29. *Guía para la notificación de brechas de datos personales*. 2021.

30. *GDPR-Subject Access Request Process and Procedure*. 2023.

31. *PROCEDIMIENTO DE EJERCICIO DE DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA*. Spain, 2024.

32. *DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO*. 2017.

33. COMISIÓN EUROPEA. *DECISIÓN DE EJECUCIÓN (UE) 2021/915 DE LA COMISIÓN*. 4 June 2021. Unión Europea.

34. COMISIÓN EUROPEA. *DECISIÓN DE EJECUCIÓN (UE) 2021/914 DE LA COMISIÓN*. 4 June 2021.

35. *ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD)*. 2019.

36. *Europrivacy G-EUROPRIVACY GDPR CORE CRITERIA*. [no date].
37. *Plan estratégico 2025-2030* Online. 2025. Available from: www.aepd.es

Anexo I: Sistema de gestión de la privacidad

Este trabajo consiste en el desarrollo de un sistema de gestión para facilitar la implantación del Reglamento General de Protección de Datos en el pequeño comercio. Esta memoria repasa el proceso de creación del sistema. Además, expande ciertos puntos y proporciona ejemplos concretos con el objetivo de servir de guía complementaria.

Por tanto, proporcionamos un enlace público[28] de solo lectura que permite acceder al sistema de gestión desarrollado. Este sistema puede ser descargado y utilizado por cualquier negocio. Este sistema se comparte bajo licencia MIT.

El contenido del sistema de gestión y los ejemplos incluidos en esta memoria no constituyen una actividad de consultoría ni asistencia legal. Cualquier uso del sistema o de los ejemplos deberá ser validado por personal cualificado. Cualquier incorrección contenida será únicamente responsabilidad del responsable del tratamiento que utilice el sistema sin la debida revisión y adaptación a las particularidades del negocio.

[28] Sistema de gestión de la privacidad https://upvedues-my.sharepoint.com/:f:/g/personal/joculde_upv_edu_es/Esi1MuGwWZtJmNSUlA4A6r8BgSwr6SsjomLbdbO6l-aS-Q?e=vg3pl2

Anexo II: Objetivos de desarrollo sostenible

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

En la introducción de este trabajo se destacó el papel del pequeño comercio como uno de los pilares fundamentales de la economía. Es por esto por lo que creemos que este trabajo puede tener un alto impacto en el objetivo de desarrollo sostenible número ocho. El pequeño comercio tiene un papel fundamental en el crecimiento económico de las naciones. Es difícil imaginar una economía en la que se crean empresas con cientos de empleados y miles de millones de ingresos desde el primer día. Todo negocio parte de una idea que se materializa en una pequeña empresa, con escasos recursos económicos y un número reducido de empleados. Con el tiempo estos negocios pueden florecer, pasando de ser un negocio con un puñado de clientes y menos de cinco empleados a grandes negocios que aportan un inmenso valor a sus clientes y dan trabajo a miles de personas de manera directa. Además, este tipo de negocios no solo tienen un impacto directo en la economía si no que sus necesidades se transmiten por toda la economía, generando redes de proveedores y decenas de miles de puestos de trabajo adicionales. Al margen de los efetos tangibles que estos negocios generan mediante el crecimiento económico y la creación de puestos de trabajo estables, podemos encontrar efectos intangibles de segunda ronda. En muchos casos, estos negocios pueden convertirse en referentes para muchas personas que busquen seguir el mismo camino, creándose un proceso de retroalimentación positiva que permite impulsar el crecimiento agregado de la economía de todo un país.

Sin embargo, en todo proceso de desarrollo económico existe el riesgo de que los beneficios del crecimiento no alcancen a todos los ciudadanos. Esto, generalmente, se debe a la falta de oportunidades que genera desigualdad. En general, existen muchos factores que pueden generar la falta de oportunidades, pero sin duda uno de ellos es la dificultad para la creación y el desarrollo de negocios que aporten una visión distinta a lo ya existente en el mercado. Uno de estos factores es la carga regulatoria a la que se ven sometidos los pequeños negocios, en particular el pequeño comercio. La carga regulatoria establece los recursos mínimos necesarios para desarrollar un nuevo negocio. Cuanto más elevada sea esta, mayor será el coste de establecer un nuevo negocio. Sin embargo, las grandes empresas ya existentes cuentan con recursos suficientes para hacer frente a todo tipo de regulaciones por lo que no suelen verse afectadas. En consecuencia, las grandes empresas son capaces de adaptarse a estos cambios, mientras que el pequeño comercio enfrenta costes más elevados que, en ciertos casos, pueden llevarlos a la quiebra. A largo plazo, la menor creación de nuevos negocios puede provocar la falta de competencia y dinamismo necesarios para mantener a las grandes empresas a raya, evitando abusos de su poder de mercado. Este proceso puede dar lugar a peores condiciones laborales, menores ingresos y oligopolios en los que una parte de la sociedad concentra una mayor cantidad de recursos que el resto, incrementando la desigualdad. Este trabajo busca reducir este el coste regulatorio, contribuyendo a incrementar las oportunidades para la creación de nuevos negocios. De esta forma, la economía seguirá funcionando óptimamente, incluyendo al mayor número posible de participantes y reduciendo las desigualdades. Esto es en definitiva lo que pretende el objetivo de desarrollo sostenible número diez.