Universidad Politécnica
de Madrid

Escuela Técnica Superior de
Ingenieros Informáticos

Grado en Administración y Dirección de Empresas

Trabajo Fin de Grado

Plan de Negocio para una Aplicación de Seguridad de Datos

Autor: Raquel Pérez López

Tutor(a): Bárbara Soriano Martínez

Madrid, Enero 2025

Este Trabajo Fin de Grado se ha depositado en la ETSI Informáticos de la Universidad Politécnica de Madrid para su defensa.

Trabajo Fin de Grado
Grado en Administración y Dirección de Empresas
Título: Plan de negocio para una aplicación de Seguridad de Datos
Mes Año

Autor: Raquel Pérez López

Tutor:
Bárbara Soriano Martínez
Economía agraria, estadística y gestión de empresa, de la Escuela Técnica Superior de Ingeniería Agronómica, Alimentaria y de Biosistemas (ETSIAAB)
Universidad Politécnica de Madrid

Resumen

En este proyecto se presenta un plan de negocio para una aplicación de seguridad de datos. Se propone la estrategia e implementación de una aplicación de seguridad de datos dirigida a startups o nuevas empresas tecnológicas interesadas en proyectos novedosos en el ámbito de la ciberseguridad. Este proyecto se enfoca en un nicho de mercado en crecimiento: la protección de datos para pequeñas y medianas empresas (PYMES), que a menudo carecen de los recursos necesarios para implementar soluciones avanzadas. El modelo de negocio se desarrolla mediante el marco Canvas Social, una herramienta que permite analizar de forma estructurada el mercado objetivo, los servicios a ofrecer, los canales de distribución, las estrategias de comunicación y la inversión requerida.

El mercado objetivo se encuentra en el sector de la ciberseguridad y tecnología, un ámbito en crecimiento exponencial impulsado por la digitalización global y el aumento de ciber amenazas. Las empresas están obligadas a cumplir con el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica 3/2018 (LOPDGDD), normativas que garantizan la seguridad y privacidad de los datos personales, pero cuya implementación puede ser compleja y costosa sin las herramientas adecuadas. La aplicación aborda esta brecha proporcionando una solución integral de bajo coste y alta calidad que combina tecnología avanzada y asesoramiento legal. Sus principales funciones incluyen: el cumplimiento normativo certificado colaborando con asesorías legales; generación de formularios y plantillas personalizadas de consentimiento, incluyendo la gestión de cookies y DPIAs (Data Protection Impact Assessments), y la clasificación, protección y monitorización de datos sensibles mediante herramientas de Microsoft, que ofrecen servicios como cifrado avanzado y prevención de pérdida de datos.

Los colaboradores son servicios software, lo que implica que no se compra y contratan instalaciones o bienes con gastos fijos. Específicamente, trata con onetrust y Microsoft. Utiliza servicios en la nube que, al ser usados para diferentes empresas con los mismos recursos, minimiza los costes, asegurando la seguridad en unos recursos compatibles para todas las empresas y distribuibles reduce los gastos sin repercusión a la calidad del servicio. Por una parte, onetrust permite realizar formularios consentimiento tanto generales como de cookies, registrar todos los datos personales que administra la empresa y generar DPIAs (Data Protection Impact Assessment). Por otra parte, los servicios de Mirosoft permiten la clasificación, monitorización y protección de datos sensibles e implementar reglas para impedir su pérdida además de cifrar los datos con un mayor nivel de seguridad. Combinando estos dos servicios con asesorías legales que ofrecen certificaciones consigue ofrecer un servicio completo y de calidad a un bajo coste.

En cuanto a la financiación, el proyecto se apoya en una combinación de fondos propios (cuarenta por ciento), préstamos bancarios (sesenta por ciento). Respecto a las tarifas del servicio, se ofrecerán cuatro para garantizar una oportunidad de compra a aquellas empresas con menos recursos y una solución más completa a aquellas con un mayor presupuesto cubriendo todos los requisitos del GDPR.

La aplicación ofrece una solución de alta calidad y asequible, diseñada para ser percibida como sencilla y fácil de implementar, adaptándose a las necesidades específicas y al presupuesto de las pequeñas y medianas empresas.

Abstract

This document develops a business plan for a data security application. It proposes the strategy and implementation of a data security application aimed at startups or new tech companies interested in innovative projects within the field of cybersecurity. The project focuses on a growing market niche: data protection for small and medium-sized enterprises (SMEs), which often lack the resources to implement advanced solutions. The business model is built using the Social Canvas framework, a tool that enables a structured analysis of the target market, services offered, distribution channels, communication strategies, and required investment.

The target market is in the cybersecurity and technology sector, an area experiencing exponential growth driven by global digitalization and the rise of cyber threats. Companies are required to comply with the General Data Protection Regulation (GDPR) and Organic Law 3/2018 (LOPDGDD), regulations that ensure the security and privacy of personal data but whose implementation can be complex and costly without appropriate tools. The application addresses this gap by providing a comprehensive, low-cost, high-quality solution that combines advanced technology with legal advice. Its main features include certified regulatory compliance through collaboration with legal advisors; generation of personalized consent forms and templates, including cookie management and Data Protection Impact Assessments (DPIAs); and classification, protection, and monitoring of sensitive data using Microsoft tools that offer advanced encryption and data loss prevention services.

The project relies on software services, which means no fixed assets or installations are purchased or contracted. Specifically, it collaborates with Onetrust and Microsoft. It uses cloud services that, by being shared across different companies with the same resources, minimize costs while ensuring security with scalable and compatible solutions that reduce expenses without affecting service quality. On one hand, Onetrust enables the creation of consent forms (general and cookie-specific), registration of all personal data managed by the company, and generation of DPIAs. On the other hand, Microsoft services allow for the classification, monitoring, and protection of sensitive data, implementation of rules to prevent data loss, and encryption with higher security standards. By combining these two services with legal advisory services that provide certifications, the project delivers a complete and high-quality service at a low cost.

In terms of financing, the project relies on a combination of self-funding (40%) and bank loans (60%). Regarding service fees, four pricing tiers will be offered to ensure affordability for companies with fewer resources while providing a more comprehensive solution for those with larger budgets, covering all GDPR requirements.

The application offers a high-quality, affordable solution designed to be perceived as simple and easy to implement, tailored to the specific needs and budgets of small and medium-sized enterprises.

Tabla de contenidos

Índice de figuras

Índice de tablas

1 Introducción

Las empresas tratan con datos privados de sus clientes como números de DNI o tarjetas bancarias frecuentemente. La información que pueden almacenar, el tiempo límite que pueden almacenarla y la seguridad con la que deben hacerlo está regulado en el Reglamento (UE) 2016/679 Del Parlamento Europeo Y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Es en este reglamento, complementado en España por La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) aprobada en 2018, donde se establece que las empresas deben recopilar, almacenar y procesar los datos personales de forma segura.

Consecuentemente las empresas españolas deben tener categorizados y protegidos todos los datos. El incumplimiento de esta protección por parte de las empresas supone:

- El incumplimiento de la normativa de protección de datos, lo que implica multas por aalmacenamiento indebido de datos o falta de medidas técnicas y organizativas para proteger la información. Estas sanciones pueden llegar a suponer hasta veinte millones de euros. (Unión Europea, 2016)
- Falta de protección ante brechas de seguridad. Lo que supone una pérdida de confianza de los clientes, obligación de informar a los afectados y a la Agencia Española de Protección de Datos (AEPD) y potenciales demandas colectivas de los clientes afectados.

Actualmente, la protección de datos es una necesidad a nivel internacional para evitar brechas por ataques de ciberseguridad, en concreto en España en 2022 el gobierno documentó un total de 374.737 hechos conocidos de ataques en ciberseguridad. Además, en la ilustración se puede observar como cada año esta cifra aumenta, en concreto, esta cifra supone un 22,67% más que el año anterior. Esto refleja que la necesidad frente a la protección en ciberseguridad es importante y aumenta anualmente.

Figura 1: Evolución global de hechos conocidos, esclarecidos y detenciones / investigados (Secretaría de Estado de Seguridad, 2022)

El objetivo de este trabajo es desarrollar el plan de negocio de una herramienta que resuelva la gestión de seguridad de datos en las pymes españolas y definir un plan de negocio para su lanzamiento al mercado para que cualquier pequeña empresa en España pueda implantarla. Los objetivos específicos son:

1. Realizar un estudio de mercado de los servicios de seguridad de datos en España
2. Elaborar un plan de negocio

La aplicación propuesta se llamará Tecnologías ProtecccionData, se desarrollará en una sede establecida en Madrid y ofrecerá servicios en toda España. Esta aplicación busca proteger a pequeñas y medianas empresas de los crecientes ataques en ciberseguridad a un precio accesible. Para ello, para todas las empresas que soliciten los servicios se utilizará la tecnología de Microsoft. Se pretende aprovechar al máximo los recursos que ofrece Microsoft Azure para grandes empresas, estandarizando los protocolos e implantándolos en cada uno de los clientes. Esto es posible mediante la sistematización de procesos en Data Loss Prevention (DLP) y Cloud Access Security Broker (CASB) dentro de la plataforma Microsoft Defender.

Para llevar a cabo este plan de negocio se utilizará la metodología Canvas Social, que guía un plan de negocio e incluye una mejora social que aporta el proyecto. En el plan se realiza la propuesta y estrategia de desarrollo de la aplicación, pero no implica la creación de una nueva empresa, ya que se contempla la opción de que una pequeña o mediana empresa tecnológica la implante.

2 Metodología

En este capítulo se explicarán las dos metodologías que se siguen en el proyecto: un análisis PESTEL y Canvas Social.

2.1 Metodología: Análisis PESTEL

El análisis PESTEL es una herramienta utilizada para identificar las fuerzas externas a nivel macro que influyen sobre un negocio y pueden determinar su evolución, tanto en términos económicos como de reputación. El acrónimo PESTEL se refiere a los factores que se analizan: Políticos, Económicos, Sociales, Tecnológicos, Ecológicos y Legales. (ESERP, 2022)

Este tipo de análisis será utilizado durante el proyecto para hacer parte del estudio de mercado.

2.2 Metodología Canvas Social

El Canvas Social es una herramienta para realizar planes de negocio analizando primero la parte cualitativa, el mercado objetivo, el valor que se ofrece y la estrategia operativa y luego la parte cuantitativa que evalúa costes de negocio. Además, no solo considera el valor económico sino también el valor social y ambiental.

Figura 2: Plantilla modelo de Canvas social (Triquels, 2020)

Como se puede apreciar en la imagen, además de ser una metodología que aporta el orden en el que seguir trabajando es una guía visual. Divide el estudio en cuatro preguntas básicas: ¿A quién? ¿Qué? ¿Cómo? ¿Cuánto? De esta forma simplifica el proceso y aporta una mayor precisión en la descripción de la actividad económica en un orden organizado. A lo largo de este proyecto se resolverán todos los objetivos siguiendo el orden de esta metodología, es decir:

1. Segmentos de Clientes: se seleccionará un segmento específico, identificando sus necesidades y cómo cubrirlas. Se planteará generar valor social, como enfocarse en empresas con menor nivel de beneficio. Esto se realizará mediante un estudio de mercado previo detallado en el siguiente apartado.

2. Propuesta de Valor: Basado en el estudio de mercado ya mencionado, se ofrece algo que diferencie a la aplicación de la competencia y cubra necesidades específicas. En este caso se buscará la mayor accesibilidad posible como parte social del Canvas

3. Relación con Clientes: definir cómo se realiza la comunicación con los clientes, sabiendo quiénes son y qué les ofrece la aplicación.

4. Canales de Distribución: estudiar la logística para llevar la aplicación a las distintas empresas y darse a conocer. En concreto, al ser una aplicación en vez de un equipo completo permite reducir la infraestructura reduciendo la contaminación de los equipos físicos en cada empresa que deben ser renovados.

5. Colaboradores: Identificar socios clave para mejorar el negocio, se establecerán proveedores o aliados estratégicos. En este apartado también se incluirá un estudio de los posibles proveedores y se justificará la elección.

6. Actividades Clave: Definir las actividades necesarias para desarrollar la aplicación y dar servicio. En este caso, como valor social se encuentra el llegar a sectores vulnerables como son empresas en riesgo de sufrir filtraciones de datos por ataques de ciberseguridad.

7. Recursos Clave: Identificar los recursos materiales y humanos esenciales para el proyecto. Se priorizará contratar personal de inserción.

En resumen, siguiendo esta metodología se obtiene una guía en la cual basar la evolución de la idea del plan de negocio.

3 Estudio de mercado de servicios de seguridad de datos

La aplicación ofrece un servicio de Seguridad de Datos, es decir, se encuentra en el sector de la ciberseguridad. En este capítulo se estudiará el mercado de la ciberseguridad, su tamaño, expectativas a futuro y competencia.

La ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados.

La demanda del mercado de ciberseguridad está creciendo anualmente debido a diferentes factores: el crecimiento exponencial de los datos, con el crecimiento del mundo digital cada día se generan e incrementan los datos disponibles, se calcula que em 2025 se alcancen los 180 Zettabytes; El crecimiento de las operaciones digitales que de 2019 a 2020 ya crecieron un 40% y surge una necesidad de hacer seguras todas ellas; El incremento de ciber amenazas, no solo directas sino a través de virus o fugas de datos difíciles de averiguar, como se apreciaba en la figura 1, los ciberdelitos aumentan cada año y también su nivel de sofisticación; El teletrabajo, tras la pandemia del COVID-19 el uso de las tecnologías y transmisión online de información ha aumentado, y con ello la necesidad de protegerla. Por todos estos motivos, el mercado ha aumentado, en 2020 el tamaño del mercado de la seguridad alcanzó los 1.479,13M€ y en 2024 se calcula en 2.021M€, un 8,12% más grande. (IDC, 2021)

Como se puede apreciar en la figura 3, todos los grupos tecnológicos han aumentado de tamaño, lo que significa que según los datos del ODC el mercado de la ciberseguridad experimentara un crecimiento en todos los sectores productivos.

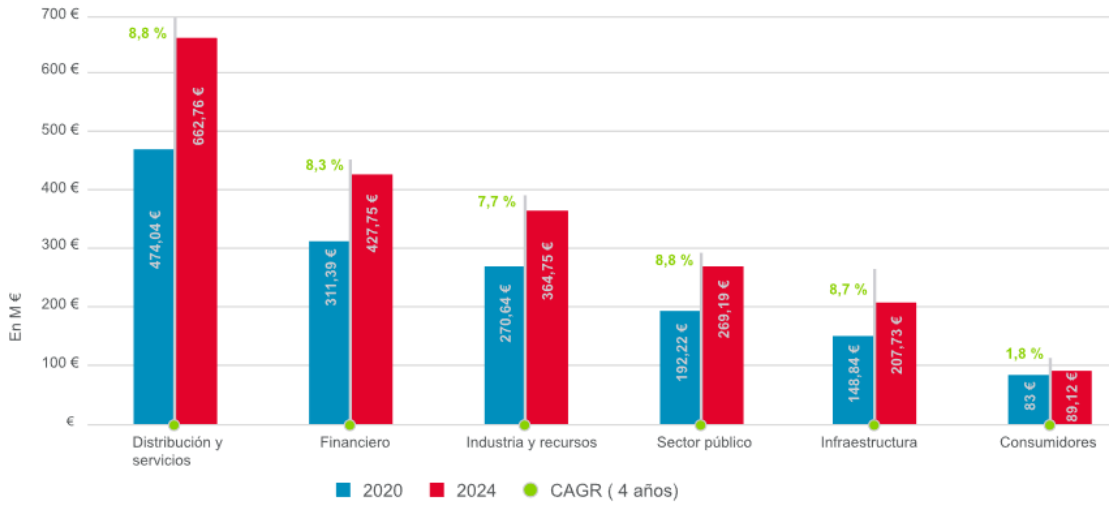

Figura 3: Tamaño de mercado por grupo de tecnología (IDC, 2021)

Este aumento del tamaño de mercado implicará una mayor demanda de servicios y soluciones como la que ofrece la aplicación; la expansión de clientes potenciales, las empresas con sin soluciones o con soluciones ineficientes cada vez es mayor, lo que se transforma en una ampliación de posibles clientes; oportunidades de alianzas estratégicas en el mercado, surge la posibilidad de establecer colaboraciones con empresas del mismo sector que busquen expandir su alcance; un aumento de la percepción de valor, al ser cada vez más

empresas las que necesitan de este servicio; mayor posibilidad de financiación, al ser un sector con oportunidades crecientes.

En cuanto a las empresas que están interesadas en ciberseguridad, no todas buscan una solución con el mismo nivel de complejidad y madurez. En concreto, hay una diferencia importante en cuanto al tamaño de la entidad en cuestión.

Como se observa en la figura 4, el mercado entre las pequeñas empresas presenta un bajo nivel de adopción, serán los particulares quienes tomarán la iniciativa para implementar medidas de ciberseguridad. En el caso de las medianas y grandes empresas, el grado de madurez en este ámbito sigue siendo bajo-medio, lo que indica la existencia de un segmento del mercado con potencial para atraer clientes interesados en nuestra aplicación.

	Particular.	Pequeñas empresas	Medianas y Grandes Empresas industriales	Infraest. Críticas no industrial.	Infraest. Críticas	Defensa interior
			IBEX 35			
EJEMPLOS	-	-	Automoción, téxtil, distr alimentaria	Serv finacieros	Energía, aerospacial.	Policía Nacional, Guardia Civil
NIVEL MADUREZ	MUY BAJO	BAJO	BAJO-MEDIO	ALTO	ALTO	MUY ALTO
DECISOR	PARTICULAR	PARTICULAR/ DG	DG/ DIR.PLANTA/ CISO	DG/ CISO	DG/ DIR.PLANTA/ CISO	CISO/ DESARR. INTERNO

Figura 4: Tipos de clientes en el mercado de Ciberseguridad (INCIBE, Análisis y caracterización del mercado de Ciberseguridad)

Estas condiciones presentan oportunidades para la aplicación, que puede posicionarse como una solución accesible y efectiva para pequeñas empresas, al tiempo que ofrece a medianas organizaciones un enfoque adaptado a su nivel de madurez en ciberseguridad. Además, estas empresas sufren efectos negativos por la ausencia de protección contra la ciberdelincuencia, lo que genera interés en aplicaciones como la propuesta.

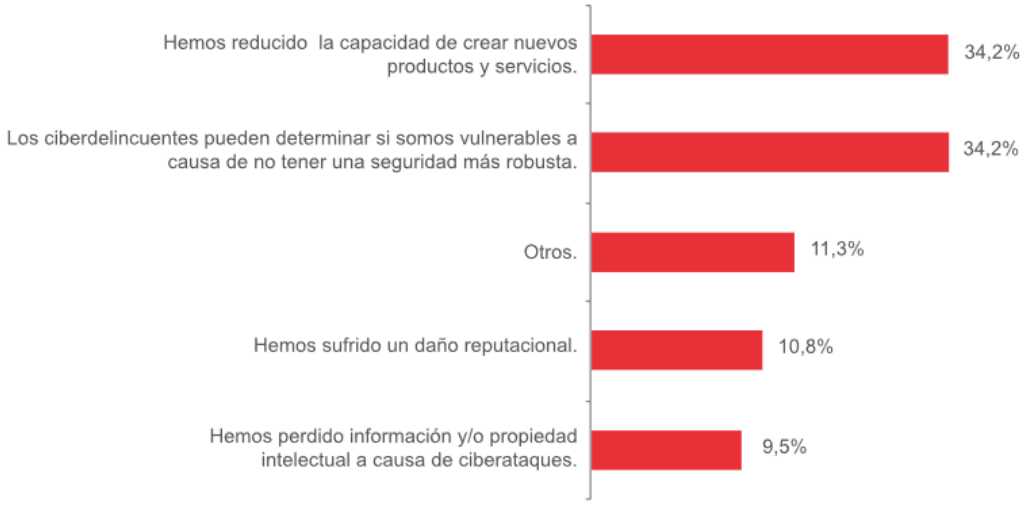

Figura 5: Principales efectos negativos de la escasez de talento de ciberseguridad en las empresas (INCIBE, Análisis y diagnóstico del talento de ciberseguridad en España, 2022)

En cuanto a la oferta, es más difícil de estudiar que la demanda. Para tener una idea aproximada se usa un informe del Iinstituto Nacional de Ciberseguridad publicado en 2024 como base, en el cual, a partir de los graduados, encuestas a empresas y datos sobre los puestos actuales en departamento de ciberseguridad comparan la oferta y demanda de este mercado.

En la tabla 1 se refleja la amplia diferencia entre oferta y demanda en el mercado de la ciberseguridad, lo que confirma el sector como una buena opción a la hora de desarrollar un negocio. Esta notable diferencia permitirá que la aplicación, una vez capte el sector de clientes especifico al que quiere llegar tenga más posibilidades de captación y potencial de crecimiento.

	2021	**2022**	**2023**	**2024**
Oferta	39.072	41.123	41.677	42.283
Demanda	63.191	67.147	74.904	83.007

Tabla 1: Proyecciones de oferta y demanda de talento en ciberseguridad en España. (INCIBE, Análisis y diagnóstico del talento de ciberseguridad en España, 2022)

Con un crecimiento anual del 8,12% y un desbalance significativo entre oferta y demanda de talento, el sector ofrece oportunidades para captar clientes, establecer alianzas estratégicas y desarrollar soluciones accesibles y adaptadas a las necesidades de PYMES.

3.1 Análisis PESTEL

Como resultado de la aplicación de la metodología PESTEL a continuación se presentan los principales factores que definen el mercado:

Factores políticos

En cuanto a la política en España sobre Seguridad de datos, las empresas se rigen por el Reglamento General de Protección de Datos (RGPD), que es el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, aprobada el 5 de diciembre de 2018 (LOPDGDD) y demás normativa nacional que sea de aplicación.

El gobierno de España busca la evolución de la ciberseguridad y Seguridad de Datos en España. Una prueba de esto es la estrategia nacional de ciberseguridad en 2019, donde se proporciona una visión de la ciberseguridad conjunta a nivel nacional, determinando las principales amenazas, la estructura orgánica en el sistema de seguridad nacional y las líneas de acción a seguir. También se ha emitido el Plan España Digital 2025, siendo uno de los objetivos reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial (meta 2025: 20.000 nuevos especialistas en ciberseguridad, IA y Datos) (España, s.f.). Además, ha lanzado el proyecto ACTIVA Ciberseguridad, un programa que ofrece un análisis de la situación actual de la empresa en materia de ciberseguridad para conocer su nivel de seguridad y la elaboración de un Plan de Ciberseguridad específico para la misma con un diseño personalizado de acciones de mejora de ciberseguridad para PYMES. (IndustriaConectada4.0,

s.f.). Otro ejemplo es el programa INCIBE emprende ofrece191 millones de euros para emprendedores y start-ups de ciberseguridad.

Factores económicos

Económicamente, la aplicación se lanza en un sector en crecimiento con grandes oportunidades de negocio en el que cada año se invierte más dinero tanto privado por las propias empresas como público en forma de ayudas.

El mercado de la ciberseguridad ha aumentado, en 2020 el tamaño del mercado de la seguridad alcanzó los 1.479,13M€ y en 2024 se calcula en 2.021M€, un 8,12% más grande. Esto implica que la demanda aumenta progresivamente y con ello los posibles clientes.

Según los datos del Informe de Ciberpreparación de Hiscox 2023 la mediana del gasto en ciberseguridad ha crecido un 39% en los últimos tres años, hasta alcanzarlos 142.600€. En las empresas con menos de diez empleados esta cifra se ha cuadruplicado en dos años. Esto es otro indicador de que la cantidad de dinero invertida en este sector aumenta anualmente.

A nivel de puestos de trabajo, *España podría alcanzar una fuerza laboral en ciberseguridad cercana a los 122.284 trabajadores con una brecha de talento que se estima en 24.119* (INCIBE, Análisis y caracterización del mercado de Ciberseguridad) , lo que confirma que el crecimiento del mercado también lleva a una subida de la oferta en el mercado laboral.

Factores sociales

Socialmente, la solución que ofrece la aplicación resuelve una gran y creciente preocupación de las empresas. El riesgo de sufrir un ciberataque aumenta cada año y las empresas reciben datos alarmantes al respecto, un ejemplo son algunas de las afirmaciones en el Informe de Ciberpreparación elaborado por Hiscox: *Los ciberataques aumentaron por cuarto año consecutivo: un 53% de las empresas sufrieron ciberataques, frente a un 48% que los sufrieron el año pasado; En tres años, el porcentaje de empresas atacadas con menos de diez empleados aumentó más de la mitad, hasta un 36%; Una de cada tres empresas atacadas sufrió pérdidas económicas debido a fraude por desvío de pagos; Una de cada ocho empresas atacadas sufrió costes de 230.000€ o más. (Hiscox, 2023)*

Todos estos datos generan malestar entre las empresas, especialmente aquellas con un bajo presupuesto para ocuparse de este tipo de ataques. La aplicación busca contactar con estas empresas y ofrecerles una solución que puedan permitirse.

Factores tecnológicos

Actualmente, la digitalización e innovación avanzan cada día. Las tecnologías evolucionan y los ataques en ciberseguridad evolucionan y se adaptan a estos cambios. Por tanto, las empresas deben mantenerse actualizadas para poder responder adecuadamente en todo momento. Esta es una tarea compleja y la aplicación propuesta lo soluciona al asumir la adaptación a estos cambios.

Cada año se producen más datos y cada vez es más complicado manejar todos. L*a cantidad de datos digitales creados o replicados a nivel mundial se ha multiplicado por más de treinta en la última década, pasando de dos zetabytes en 2010 a 64 zetabytes el año pasado. Según las previsiones, el volumen de datos generados en todo el mundo superará los 180 zetabytes en 2025, lo que supone un crecimiento medio anual de casi el 40% en cinco años* (Mónica, 2021) Esto implica que cada ver el volumen de datos a tratar en términos de seguridad

también está creciendo y necesita soluciones actualizadas como la ofrecida por la aplicación.

Factores ecológicos

El factor ecológico más importante al que puede afectar la aplicación es a la huella de carbono digital. Esta huella es el conjunto de contaminación producida por los gases de efecto invernadero debido al uso de las TIC. Las emisiones de la huella de carbono digital ya suponen entre un 1,8 y un 2,8% de las emisiones totales. (Valencia, 2021)

Algunos de los factores que aumentan la huella digital son: los centros de datos, donde se almacena de forma fisca toda la información que se maneja en internet y crece exponencialmente; El suministro eléctrico que permite la conexión a internet; Las horas de uso de dispositivos electrónicos.

Para tratar de reducirla es importante mantener el menor número de datos posible, optimizar la energía de los dispositivos, usar motores de búsqueda responsable y tratar de usar energías renovables.

Factores legales

En cuanto al tratamiento de datos personales por parte de las empresas que manejaría la aplicación, deben garantizar determinados marcos legales, específicamente el Gobierno en la página relativa a la Normativa sobre datos personales según el Ministerio de hacienda resalta:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Este reglamento regula temas como el consentimiento del usuario, derechos de acceso y rectificación de datos, y obligaciones de seguridad en el tratamiento de datos. Las empresas que incumplen pueden enfrentarse a sanciones económicas elevadas.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vigente en los artículos referidos en la Disposición adicional decimocuarta y Disposición transitoria cuarta de la Ley Orgánica 3/2018, de 5 de diciembre.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

También hay normativas que obligan a algunos sectores a implementar medidas legales en términos de ciberseguridad a las empresas como la Directiva de la UE sobre la seguridad de las redes y sistemas de información (Directiva NIS2) que afecta a sectores críticos como salud, energía, transporte, agua, y servicios financieros.

Además de las leyes y normas obligatorias, hay certificados como ISO 27001 que son estándares internacionales para la gestión de seguridad de la información, que es valorado en sectores altamente regulados. En concreto, en estos estándares se especifica los requisitos para establecer, implementar y

mantener un sistema de gestión de seguridad de la información, cubriendo también los procesos de evaluación de riesgos y control de acceso.

4 Plan de negocio

En este capítulo se realizará el plan de negocio de la aplicación siguiendo la metodología del Canvas Social explicada con anterioridad. En cada apartado del capítulo se responde a una de las preguntas clave de la metodología y cada subapartado corresponde a cada uno de los elementos a analizar.

4.1 Mercado objetivo

En este primer apartado se resolverá la pregunta ¿A quién? del plan de negocio. Para tener un contexto en este apartado, se ha introducido con anterioridad el mercado de ciberseguridad. En primer lugar, se establecerá el segmento de clientes. Posteriormente, se definirá la estrategia de comunicación para llegar a estos clientes de manera efectiva, y finalmente, se analizarán los canales de distribución adecuados para asegurar el alcance óptimo del servicio a los segmentos de clientes establecidos.

4.1.1 Segmento de clientes

El segmento de clientes al que desea llegar "Tecnologías ProtecciónData" está compuesto por pequeñas y medianas empresas (PYMES) en toda España que necesitan reforzar sus defensas en Seguridad de Datos. Como se aprecia en la figura 4, presentada anteriormente, estas empresas tienen un nivel de madurez bajo o medio-bajo en ciberseguridad. Esto significa que algunas no tienen soluciones implementadas o expertos en la empresa que puedan tomar medidas para cumplir la regulación y evitar posibles ataques, lo que supone un amplio nicho de mercado.

Como se puede observar en la figura 6, aun son muchas las empresas que carecen de un departamento propio de seguridad, un 20,5%. Estas empresas son posibles clientes de nuestra aplicación, que no tengan suficiente presupuesto como para un departamento propio de seguridad, pero sufren los efectos negativos de no tener un sistema de seguridad de datos.

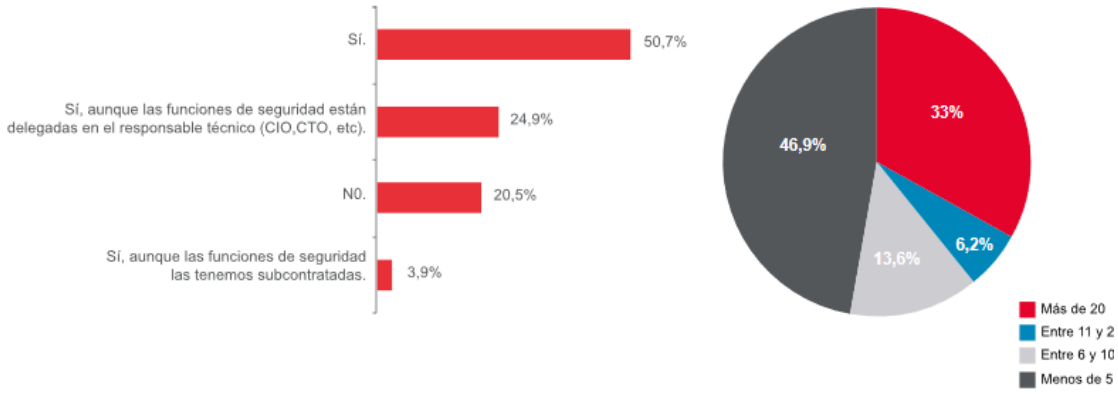

Figura 6: Existencia de departamentos de seguridad en las organizaciones (INCIBE, Análisis y diagnóstico del talento de ciberseguridad en España, 2022)

El segmento objetivo de "Tecnologías ProtecciónData" está compuesto por PYMES en España, muchas de las cuales carecen de un departamento propio de seguridad (20,5%) y enfrentan riesgos por no contar con sistemas adecuados, siendo clientes potenciales de soluciones accesibles como la ofrecida por la compañía.

Perfil Demográfico

El sector de clientes a estudiar son las pequeñas y medianas empresas (PYMES), es decir aquellas que tienen entre 0 y 249 asalariados. Actualmente en España hay 2.927.956 PYMES. En concreto, la distribución de empresas según su tamaño es la que se puede observar en la figura 7, en España suponen más de un 50% por lo que es un sector muy amplio de la población. La mayoría de las PYMES no cuentan con personal especializado en ciberseguridad, de modo que el perfil de cliente ideal busca una solución que pueda implementarse y gestionarse sin conocimientos avanzados en tecnología. Estas empresas son mayoritariamente del sector servicios, donde se trata con información privada de clientes como números de teléfono, direcciones, números de tarjetas de crédito o documentos de identidad.

En concreto, la distribución de empresas según su tamaño es la que se puede observar en la figura 7, en España suponen más de un 50% por lo que es un sector muy amplio de la población. La mayoría de las PYMES no cuentan con personal especializado en ciberseguridad, de modo que el perfil de cliente ideal busca una solución que pueda implementarse y gestionarse sin conocimientos avanzados en tecnología. Estas empresas son mayoritariamente del sector servicios, donde se trata con información privada de clientes como números de teléfono, direcciones, números de tarjetas de crédito o documentos de identidad.

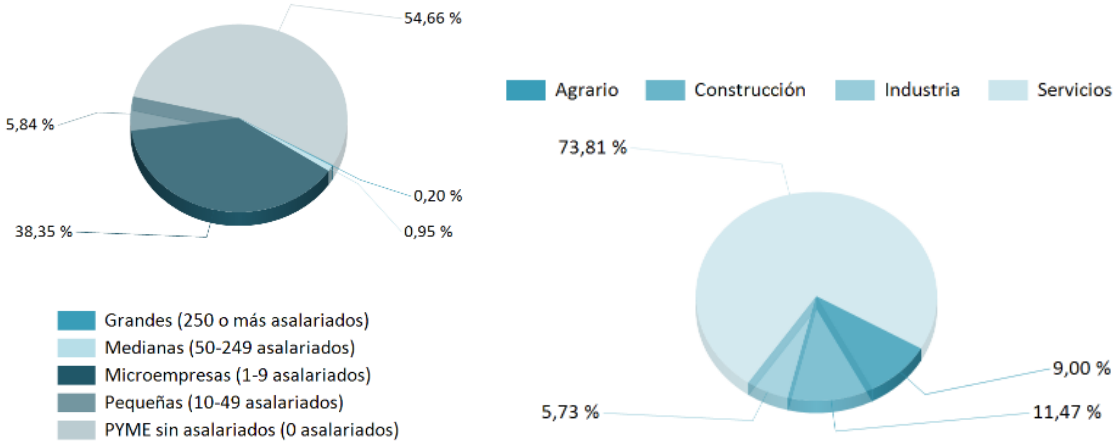

Figura 7: Distribución de Empresas por tamaño y sector (Ministerio de Industria y turismo, 2024)

Estudios del Instituto Nacional de Ciberseguridad (INCIBE) revelan que aproximadamente un 43% de las PYMES en España no disponen de personal capacitado en ciberseguridad y un 53% de las que sí tienen personal confirman que no están suficientemente preparados para enfrentar amenazas avanzadas. Teniendo en cuenta el numero actualizado de PYMES en España, esto supones aproximadamente 1,2 millones de empresas que carecen de personal capacitado en ciberseguridad.

Según el informe de Ciberpreparación de Hiscox 2023, la mediana del gasto en ciberseguridad ha crecido un 39% en los últimos tres años, hasta alcanzar los 142.600€. En las empresas con menos de diez empleados esta cifra se ha cuadruplicado en dos años. Por lo que tanto el número de empresas interesadas en estos productos como la cantidad que estas dispuestas a invertir aumenta.

Además, la compañía PWC realizó en 2024 numerosas entrevistas a directivos para el Digital Trust Survey 2024 que reveló que, entre los entrevistados, un 81% en todo el mundo y 82% en España prevén aumentar sus inversiones en

ciberseguridad. En nuestro España, un 48% calcula el incremento entre el 6% y el 15%, respecto al año anterior.

Desde el enfoque del impacto social, se contribuye a reducir la brecha tecnológica, concretamente en el campo de la ciberseguridad, entre empresas de diferentes tamaños, ofreciendo una solución accesible para las pequeñas y medianas empresas. Según el informe de Ciberpreparación de Hiscox 2023, esta brecha cada vez es más grande por la diferencia de inversión entre las empresas de distinto tamaño. En tres años, el porcentaje de empresas atacadas con menos de diez empleados aumentó más de la mitad, hasta un 36%.

4.2 Estrategia de comunicación

La estrategia de comunicación de "Tecnologías ProtecciónData" tiene como objetivo alcanzar y captar la atención de las pymes a través de canales digitales y eventos empresariales. Dado que el cliente ideal puede no tener conocimientos avanzados de ciberseguridad, es fundamental que la comunicación sea clara y explique los beneficios de manera accesible:

Estrategia de Comunicación digital

En esta campaña, se busca conseguir una serie de anuncios en redes sociales e internet con el objetivo de que la información de la aplicación llegue a los posibles clientes.

Este tipo de campañas digitales permite llegar a un mayor segmento de la población y ser percibida como más cercana y asequible. No obstante, este tipo de publicidad también genera desconfianza. Las aplicaciones ofertadas de forma digital son muchas y pueden consistir en estafas. La posibilidad de esta posible suplantación hace que muchas empresas no decidan dar el paso a probar las aplicaciones ofertadas. (INESDI, 2021)

Estrategia de Comunicación presencial

En esta campaña se busca mostrar con mayor nivel de detalle la aplicación, permitiendo a los clientes probarla. El objetivo es, al mostrar la aplicación en persona, ser percibida como fiable y eficiente. Para conseguirlo se buscará la presencia de un representante de la aplicación en diferentes eventos y conferencias. Además, durante el primer año se seguirá una estrategia de Prueba Gratuita Limitada. En eventos y canales de captación presencial, se ofrecerá una licencia gratuita para un taller o versión de prueba durante un mes, lo cual incluye hasta 49 cuentas de usuario por empresa. Esto permite que cada empresa implemente la herramienta sus equipos de trabajo y evalúe su utilidad de manera realista. Dado que el periodo gratuito puede suponer un coste considerable, la campaña de pruebas gratuitas se plantea solo para el primer año de lanzamiento de la aplicación. Ese año es crucial para crear una base inicial de clientes, aprovechando el impulso inicial y la visibilidad que genera la campaña. Al ofrecer un mes de prueba gratuito se elimina una de las principales barreras de entrada para PYMES con recursos limitados, facilitando el acceso a una solución que de otro modo podrían considerar de alto coste. Además, las empresas generan una relación de confianza con la marca y, si quedan satisfechas, es más probable que se conviertan en clientes recurrentes o incluso los mismos clientes pueden actuar como embajadores del producto, recomendándolo a otras empresas de su red o entorno.

Los eventos en los que se tendría presencia serían, por una parte, de captación de empresas ya interesadas en ciberseguridad dispuestas a invertir un presupuesto establecido como en talleres y seminarios de ciberseguridad o demostraciones en vivo en ferias y congresos.

También se buscará la asistencia a eventos específicos de PYMES que no tengan por qué haber realizado ya un presupuesto para ciberseguridad ni lo contemplen como prioridad. Este tipo de empresas también puede estar interesada por la mejora de la logística y seguridad que ofrece la aplicación y la mejora de imagen de marca que supone la implementación. Algunos ejemplos seria asistir a eventos de patrocinios y alianzas con entidades de apoyo a PYMES, consultoría gratuita o sesiones de diagnóstico.

4.3 Canales de distribución

Una vez aclarado el segmento de clientes objetivo, pequeñas y medianas empresas españolas interesadas en implementar un plan de seguridad de datos con un presupuesto bajo o medio-bajo. También se conoce la estrategia de comunicación a seguir. Esta estrategia tiene dos grandes canales, digitales y presenciales, cada uno con un objetivo diferente. En este subapartado se detallan los canales de distribución de estas dos campañas y del producto final.

Canales de Comunicación digitales

En esta campaña se busca llegar a un mayor segmento de la población y ser percibida como cercana y asequible. Los canales que se utilizarán serán:

1. Redes Sociales (LinkedIn, Facebook e Instagram). Por un lado, se usará LinkedIn, la principal red para profesionales y empresas. Es ideal para conectar con gerentes de empresas y profesionales interesados en ciberseguridad que ya están registrados en esta red y están pendientes de posibles ofertas, además, los anuncios patrocinados en LinkedIn permiten segmentación avanzada por industria, tamaño de empresa y cargo, facilitando la llegada a decisores de compra. Por otra parte, Facebook e Instagram se utilizarán para difundir contenido visualmente atractivo sobre la aplicación, el objetivo es que las empresas localicen la marca y puedan llegar a otras fuentes de información con contenido técnico y muestras de uso.
2. Google Display Ads: esto permite que la aplicación aparezca en los resultados de búsqueda cuando un usuario consulta temas relevantes, como “soluciones de Seguridad de datos para pymes”.
3. Plataformas de Revisión y Comparación de Software (Capterra): es una plataforma especializada donde los clientes buscan y comparan software. Puede facilitar la toma de decisiones de empresas que buscan soluciones de Seguridad de Datos, con la ventaja de que los clientes pueden leer reseñas y comparar opciones.

Canales de Comunicación presenciales

Para conseguir eficiencia en la campaña de comunicación presencial, en la cual se busca mostrar con mayor nivel de detalle la aplicación permitiendo a los clientes probarla se utilizarán diversos canales.

1. Eventos de Networking empresarial. Consiste en la participación en eventos o conferencias dirigidas a PYMES sobre tecnología y seguridad. En estos eventos también hay "networking breakfasts", donde los asistentes puedan discutir sus preocupaciones y necesidades en un ambiente más relajado. Inicialmente se acudirá a South Summit (Madrid) es un evento destacado de innovación y emprendimiento que atrae a startups, PYMES y empresas de diferentes sectores, incluyendo tecnología organizado por IE University y Spain Startup

2. Talleres y Seminarios de Ciberseguridad: charlas y talleres gratuitos organizados en asociaciones de empresarios o cámaras de comercio locales. Inicialmente se participará en *INCIBE CyberCamp*, organizado anualmente por el Instituto Nacional de Ciberseguridad (INCIBE), incluye talleres específicos de ciberseguridad para PYMES y emprendedores. Consiguiendo una aportación en este evento se muestra la aplicación como fiable y segura.
3. Demostraciones en Vivo en Ferias y Congresos: Crear un espacio interactivo en ferias de tecnología o eventos de ciberseguridad donde los visitantes puedan ver en directo cómo funciona la aplicación. Inicialmente se plantea participar en *DES - Digital Enterprise Show* (Madrid), una feria importante de transformación digital permite exponer herramientas y soluciones tecnológicas en tiempo real organizada por Nebext.
4. Patrocinios y Alianzas con Entidades de Apoyo a PYMES: Colaborar con entidades o asociaciones de apoyo a PYMES para patrocinar eventos o actividades. Esto posiciona la aplicación como una aliada confiable y refuerza la relación de la empresa con el sector, aumentando la visibilidad y el valor percibido por los asistentes. Inicialmente se plantea la asistencia y patrocinio en el *Foro de Ciberseguridad* organizado por *CEOE* (Confederación Española de Organizaciones Empresariales)

4.4 Propuesta de valor

La propuesta de valor consiste en una aplicación que ofrece servicios de seguridad de datos por un precio medio bajo a pequeñas y medianas empresas en España. Utilizando herramientas Cloud de grandes proveedores utiliza estándares modelo para clasificar datos, prevenir su perdida y protegerlos. La estandarización de este proceso permite exportarlo a distintas empresas pequeñas a un precio asequible. De esta forma distintas empresas con presupuesto limitado pueden proteger tanto sus datos sensibles como los de sus clientes cumpliendo la normativa actual.

Hoy en día la regulación de Seguridad de Datos Europea es densa y difícil de cumplir. No obstante, todas las pequeñas y medianas empresas con recursos limitaos están obligadas a aplicarlo. Esta aplicación ofrece una solución de protección de datos que verifica el cumplimiento de la regulación asegurando la protección de datos a sus clientes y ante posibles problemas legales.

Además, al ofrecer una solución para cumplir la normativa actual de protección de datos reduce el riesgo de sufrir un ciberataque. El Informe Digital Trust Survey 2024 revela que el 43% de los entrevistados en España asegura que la seguridad en la nube es su principal preocupación en materia de ciber riesgos y el 82% tienen previsto aumentar sus inversiones en ciberseguridad. De esta forma, la aplicación cubre la necesidad de las empresas de protección de Seguridad de Datos ante posibles brechas de seguridad o ataques maliciosos.

Es una solución accesible, una herramienta intermedia que evita la ausencia de protección ante posibles pérdidas de datos sensibles sin necesitar un equipo especifico de seguridad de datos. La estandarización de políticas y ausencia de particularidad hacen posible una reducción en los costes que vuelve la aplicación atractiva para empresas con menor presupuesto.

Ofrece monitorización continua. Las políticas de prevención de perdida de datos definidas son las que garantizan la seguridad. La tecnología detrás de estas políticas consiste en, bloqueos, alertas y monitorización continua tanto de

archivos en la nube como acciones de los usuarios como descargas y envíos de información.

Además, tiene una gran facilidad de uso. El usuario no necesita conocimientos específicos sobre la tecnología y políticas detrás de la aplicación. Al consistir principalmente en aplicación de políticas ya diseñadas el usuario no necesita realizar acciones continuas o espontaneas para garantizar la seguridad de datos. Para comprobar los resultados y estadísticas se comprueban informes de actualización continua.

4.5 Estructura operativa

En este apartado se analizará la estructura operativa del proyecto, la cual constituye el conjunto de colaboradores, recursos y actividades que permiten lanzar la aplicación.

4.5.1 Colaboradores

El primer colaborador es onetrust, una plataforma que permite que puedas recopilar, controlar y usar los datos con una visibilidad y control completos. Tiene diferentes apartados que recopilan datos de clientes e interesados en una compañía cumpliendo con la normativa actual. Para esto dispone de distintos apartados:

- Consent & Preferences: simplifica la gestión de las preferencias y el consentimiento para conseguir transparencia de cara al consumidor. Por un lado, ofrece a los usuarios que elijan preferencias, sobre qué quieren dar su consentimiento a partir de un portal único e intuitiva, recoge esta información con su consentimiento y administra el consentimiento de las cookies en tus sitios web, aplicaciones móviles, aplicaciones OTT y CTV.
- Privacy Automation: permite el uso responsable durante todo el ciclo de vida de los datos al operacionalizar el programa de privacidad. Automatiza todo el proceso para gestionar las solicitudes de derechos de los interesados, desde la recepción y verificación de identidad, hasta la identificación y localización de los datos, su eliminación o modificación, y la entrega de una respuesta segura. Permite visualizar flujos de datos, localiza y clasifica activos, evalúa los riesgos de privacidad en tiempo real y administra de manera eficiente los incidentes y avisos de privacidad.
- Data & AI Governance: descubre qué datos tienes y dónde, cuáles de estos son confidenciales y a qué riesgos se enfrenta tu negocio.
- Tech Risk & Compliance: supervisa del cumplimiento normativo en la organización. Simplifica los requisitos regulatorios dividiéndolos en elementos claros y medibles. Conecta los controles técnicos, las evidencias y las obligaciones legales con un lenguaje accesible para el ámbito empresarial.
- Third-Party Management: automatiza la gestión de terceros desde su incorporación hasta la evaluación, mitigación, monitorización continua y la creación de informes de riesgos.
  (onetrust, s.f.)

Por otra parte, se van a utilizar los servicios de Microsoft para la clasificación, monitorización y prevención de pérdida de datos. Microsoft Purview ofrece diferentes servicios para cubrir estas necesidades, en concreto se utilizarán:

- Microsoft Purview para clasificación y etiquetado. Primero para la identificación de datos sensibles usa sensores de clasificación automática, que detectan tipos de información confidencial preconfigurados (como nombres, direcciones, números de identificación)

también dispone de una opción para configurar etiquetas personalizadas y etiquetado manual.
- Microsoft Purview para una monitorización continua, en concreto la opción de mapa de datos (Data Map) para rastrear dónde se encuentran los datos sensibles en tiempo real. También permite habilitar informes automatizados para auditar el acceso, la manipulación y la exposición de los datos sensibles.
- Microsoft Purview para la prevención de datos con la herramienta Data Loss Prevention (DLP) para proteger los datos sensibles y evitar su pérdida o exposición no autorizada, tanto dentro como fuera de la organización.

También se usará Microsoft Compliance Manager para asegurar el cumplimiento normativo. Esta herramienta permite realizar evaluaciones de cumplimiento específicas del reglamento GDPR o LOPDGDD. Para esta evaluación permite tanto utilizar plantillas preconfiguradas para identificar brechas y generar un plan de acción como documentar pruebas de cumplimiento automáticamente, como configuraciones de políticas y logs de acceso.

Además, se fomentará Sharepoint como medio para compartir información ya que permite tanto cifrado en tránsito, por el cual los datos están protegidos mientras viajan entre el usuario y el servidor, como el cifrado en reposo, donde la información almacenada está protegida contra accesos no autorizados.

4.5.2 Actividades Clave

En este apartado se van a presentar el desglose de las actividades de la aplicación y de su lanzamiento.

Actividades clave del servicio

La actividad clave es la gestión y protección de los datos de las empresas. En primer lugar, es necesario entender que es la gestión de un dato, es decir, recopilar, mantener y utilizar datos de manera segura. Para conseguir llevar esto a cabo es necesario entender el ciclo de vida de los datos.

- Primera etapa: Creación de datos. Los datos se crean o se introducen en el sistema, algo que puede ocurrir a través de diversas fuentes.
- Segunda etapa: Almacenamiento y organización. Los datos se guardan en sistemas de almacenamiento, bases de datos u otros repositorios. La estructuración y clasificación adecuadas facilitan la recuperación eficiente de la información cuando sea necesario. Las tecnologías de almacenamiento en la nube y bases de datos desempeñan un papel vital en esta fase.
- Tercera etapa: Procesamiento y análisis. Esta etapa involucra el procesamiento y el análisis de los datos para extraer información valiosa. Aquí se aplican técnicas de análisis de datos, como la minería de datos, la inteligencia artificial o el aprendizaje automático, para descubrir patrones, tendencias y conocimientos.
- Cuarta etapa: Distribución y acceso. Se distribuyen a los usuarios o sistemas relevantes. Esto puede ser mediante informes, visualizaciones, aplicaciones o cualquier medio que permita a los usuarios acceder y utilizar la información de manera efectiva.
- Quinta etapa: Retención y copia de seguridad. La retención de datos es crucial por razones legales, regulatorias y operativas. En esta etapa se establecen políticas para determinar cuánto tiempo se deben conservar

los datos en función de su relevancia y uso potencial futuro. Además, se hacen copias de seguridad para garantizar la recuperación en caso de pérdida de datos por fallos técnicos o sucesos inesperados.

- Sexta etapa: Archivado y gestión de datos históricos. Cuando los datos ya no son necesarios para operaciones diarias, se transfieren a sistemas de almacenamiento o se archivan. Así, esta etapa implica la gestión eficiente de datos históricos, permitiendo su recuperación si es necesario para auditorías, cumplimiento normativo u otros fines. En este sentido, es muy importante establecer políticas claras para el archivado y la gestión de datos históricos.
- Séptima etapa: Eliminación segura. Puesto que los datos obsoletos o que ya no son relevantes deben ser eliminados de manera segura para evitar riesgos de seguridad y cumplir con las regulaciones de privacidad. Esto implica la destrucción de datos de forma que no puedan ser recuperados, ya sea físicamente o mediante métodos de eliminación digital seguros. (ESIC, 2024)

Además, es necesario saber qué medidas es necesario aplicar para cumplir regulaciones y ofrecer un servicio seguro y en qué fases del ciclo se implementa cada una.

El Reglamento General de Protección de Datos (GDPR) establece un marco legal que protege los datos personales de los ciudadanos de la Unión Europea (UE) y del Espacio Económico Europeo (EEE) en los que se encuentran las pequeñas y medianas empresas españolas.

Los datos personales deben estar de acuerdo con los siguientes principios:

1. Licitud, lealtad y transparencia: Los datos deben ser tratados de manera legal, justa y transparente para el usuario. Se debe informar claramente sobre cómo se usarán los datos.
2. Limitación de la finalidad: Los datos deben recopilarse para fines específicos, explícitos y legítimos, y no ser tratados de manera incompatible con esos fines.
3. Minimización de datos: Recoger solo los datos estrictamente necesarios para el propósito declarado.
4. Exactitud: Asegurar que los datos sean precisos y actualizados. Los datos incorrectos deben corregirse o eliminarse.
5. Limitación de la conservación: No almacenar datos personales más tiempo del necesario para cumplir los fines declarados.
6. Integridad y confidencialidad: Garantizar la seguridad adecuada de los datos personales, incluyendo la protección contra el acceso no autorizado, pérdida o destrucción.
7. El usuario debe dar su consentimiento claro, informado y explícito.

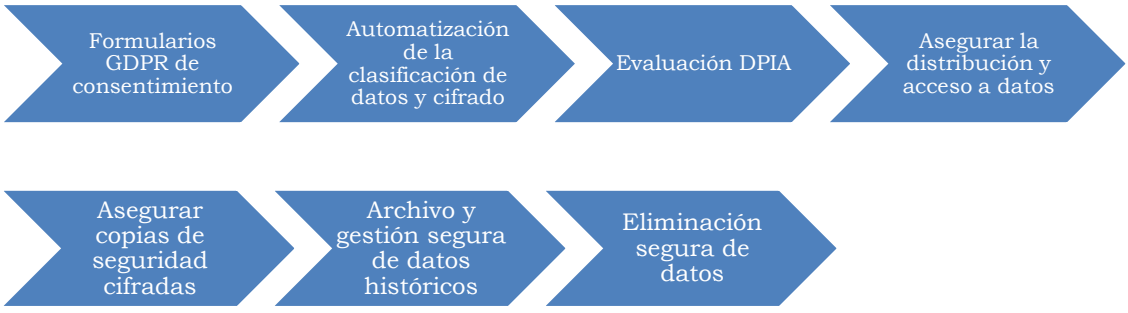

Figura 8: Etapas de la aplicación [Elaboración propia]

En la primera etapa se utilizará una herramienta para implementar formularios de recolección de datos compatibles con GDPR, incluyendo el consentimiento explícito y rastreable, configurar políticas de privacidad adaptadas a cada tipo de dato y gestionar registros de actividades de procesamiento. En este formulario, por tanto, se deben incluir los derechos de los usuarios recogidos en los artículos del doce al veintidós de El Reglamento General de Protección de Datos:

- Derecho de acceso: Los usuarios tienen derecho a saber qué datos personales se recopilan y cómo se utilizan.
- Derecho a la rectificación: Los interesados pueden solicitar la corrección de datos incorrectos o incompletos.
- Derecho al borrado: Los usuarios pueden pedir que se eliminen sus datos cuando ya no sean necesarios o si revocan su consentimiento.
- Derecho a la restricción del tratamiento: Los usuarios pueden limitar el uso de sus datos en ciertos casos.
- Derecho a la portabilidad de los datos: Los usuarios tienen derecho a recibir sus datos en un formato estructurado, de uso común y a transferirlos a otro proveedor.
- Derecho de oposición: Los usuarios pueden oponerse al tratamiento de sus datos, especialmente en marketing directo o en decisiones basadas únicamente en procesos automatizados.

Además, en esta etapa se deben etiquetar datos sensibles desde el momento de su creación y habilitar validaciones en tiempo real para garantizar que solo se recopilen los datos necesarios y permitidos.

En la segunda etapa se debe automatizar la clasificación de datos según su nivel de sensibilidad e implementar auditorías de almacenamiento para asegurar que los datos se encuentren en repositorios autorizados permitiendo monitorear accesos y alertar sobre actividades sospechosas.

También es necesario Implementar medidas de seguridad como son el cifrado, pseudonimización, control de acceso y auditorías regulares de acuerdo al artículo treinta y dos del Reglamento General de Protección de Datos. Se debe asegurar el cifrado de los datos almacenados

En la tercera etapa se deben evaluar el impacto del procesamiento (DPIA) utilizando plantillas integradas para identificar riesgos en tiempo real. Una de las obligaciones de las empresas según el artículo treinta y cinco del Reglamento General de Protección de Datos es realizar evaluaciones de impacto de este tipo cuando el procesamiento de datos pueda generar un alto riesgo para los derechos de los usuarios, como en el caso de nuevas tecnologías o procesamiento masivo.

Además, se deben implementar medidas de seguridad en este nivel de anonimización o pseudonimización antes de realizar análisis, según sea necesario.

En la cuarta etapa para la distribución y acceso se debe tener un control granular de acceso y permisos y medidas de detección y bloqueo de intentos de acceso no autorizados. Algunas soluciones que se implementarán para esto en función de las necesidades de la empresa serán:

- Establecer y aplicar controles de acceso basados en roles (RBAC) y principios de necesidad de saber
- Controlar accesos basados en identidad.

- Configurar permisos granulares en SharePoint y Teams para compartir información de forma segura.
- Aplicar cifrado de extremo a extremo para datos compartidos.

En la quinta etapa, retención y copia de seguridad, se deben realizar copias de seguridad regulares y cifradas, políticas automatizadas de retención y eliminación de datos caducados y un registro de cumplimiento para inspecciones regulatorias.

En la sexta etapa de archivado y gestión de datos históricos se debe garantizar el acceso controlado a datos archivados, almacenamiento de largo plazo con seguridad y bajo costo y la generación de reportes para auditorías regulatorias. En este caso, para llevarlo a cabo se ofrecen servicios para lo siguiente:

- Definir políticas claras de archivado alineadas con los requisitos legales y regulatorios.
- Realizar auditorías automáticas del contenido archivado para verificar que esté protegido y actualizado.
- Usar una herramienta para datos históricos cifrados.
- Configuraciones para rastrear los datos archivados y su accesibilidad.

En la Séptima etapa, eliminación segura, se ofrecerá el realizar una automatización de procesos de eliminación conforme a regulaciones, métodos seguros como el borrado criptográfico o la sobreescritura y trazabilidad y certificación del proceso de eliminación. También es importante gestionar solicitudes de borrado (derecho al olvido) a través de un portal dedicado en todo momento.

Además, la aplicación puede o bien entregar los servicios mencionados a la empresa y que esta se encargue de las gestiones o hacer la función de Delegado de Protección de Datos (DPO), obligatoria para organizaciones públicas, empresas que realizan monitoreo sistemático a gran escala y entidades que procesan datos sensibles.

También se ofrece la opción de o bien entregar los servicios mencionados a la empresa y que esta se encargue de las gestiones de violaciones de datos o que lo haga la propia aplicación. Estas consisten principalmente en notificar en caso de una brecha de seguridad que comprometa datos personales a la autoridad de control en un plazo máximo de 72 horas y a los interesados si la brecha implica un alto riesgo para sus derechos.

Actividades clave para el lanzamiento de la aplicación

Para poder lanzar esta aplicación es necesario previamente haber desarrollado los formularios de consentimiento y DPIA a implantar en las diferentes empresas. Además, también es necesario crear las plantillas base con los protocolos de Microsoft Purview cuya implantación en los sistemas de los clientes se quiere automatizar. Todos estos procesos se revisarán con una asesoría legal que certifique el cumplimiento del GDPR y se resumirá en una documentación clave y campaña digital y presencial. A continuación, se presenta un diagrama de Gantt en la figura 9 con la planificación de las tareas de lanzamiento para gestionar y visualizar el cronograma de actividades necesarias para el lanzamiento de la aplicación.

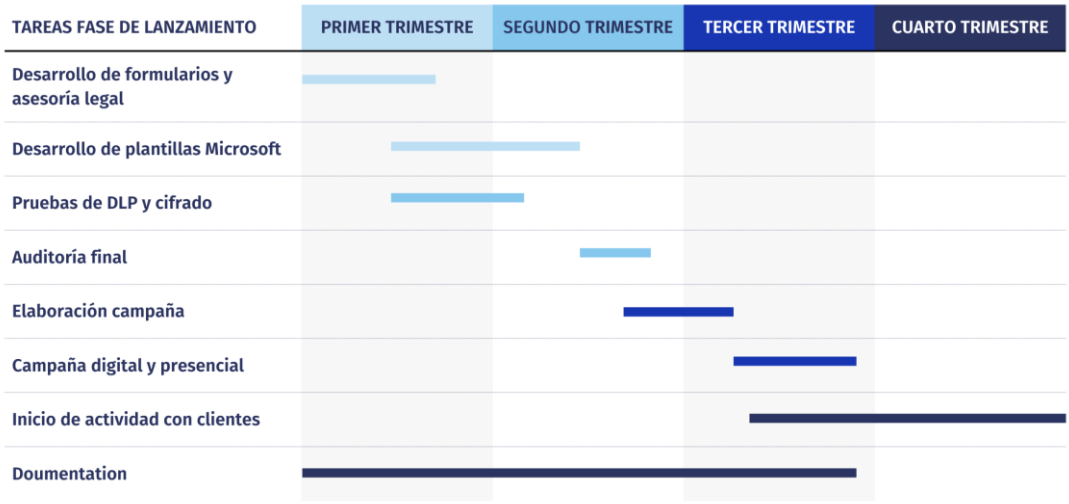

Figura 9: Diagrama de Gantt con planificación de las tareas de lanzamiento. [Elaboración propia]

Se ha establecido un plan de lanzamiento con una duración total de un año, en la cual se comienza a dar servicio a clientes a mediados del tercer trimestre. Las tareas de preparación llevarán aproximadamente seis meses. En este tiempo se diseñará la automatización de formularios y herramientas para la posterior implantación en usuarios clientes. El desglose de las tareas en etapas es el siguiente:

- Primera etapa: Desarrollo de formularios y asesoría legal (Primer trimestre). Consiste en la creación de documentos adaptados a las necesidades de recopilación de datos, consentimiento, y otros procedimientos relacionados con la GDPR. También se incluye la contratación de servicios de asesoría legal en un despacho especializado para garantizar que las plantillas y procesos cumplen con las normativas europeas de protección de datos y tener la certificación correspondiente.
- Segunda etapa: Desarrollo de plantillas Microsoft (Primer y segundo trimestre). Consiste en la creación de documentos y configuraciones predefinidas utilizando Microsoft Purview y herramientas relacionadas. En esta fase se buscará la optimización de las plantillas para facilitar su implementación por parte de PYMES.
- Tercera etapa: Pruebas de DLP y cifrado (Primer y segundo trimestre). Consiste en la implementación de políticas de prevención de pérdida de datos (DLP), validación de su eficacia y optimización de configuraciones para asegurar que las políticas no interfieran con las operaciones normales de los usuarios. Además, se realizarán pruebas para asegurar que los datos están cifrados correctamente y se cumplen las normativas.
- Cuarta etapa: Auditoría final (Segundo trimestre). Consiste en la evaluación completa del sistema antes de su lanzamiento para garantizar que cumple con todas las especificaciones técnicas y legales. Se realizarán pruebas de seguridad adicionales y una auditoría por parte de terceros si es necesario.
- Quinta etapa: Elaboración de la campaña (Tercer trimestre). Consiste en el diseño y planificación de campañas digitales y presenciales para promocionar la aplicación.

- Sexta etapa: Campaña digital y presencial (Tercer y cuarto trimestre). Consiste en la ejecución de las campañas diseñadas en redes sociales, email marketing, eventos y ferias detalladas en el apartado anterior.
- Séptima etapa: Inicio de actividad con clientes (Cuarto trimestre). Consiste en realizar pruebas piloto con los primeros clientes, permitiéndoles utilizar la aplicación y recopilando feedback. Estos primeros clientes tendrán el privilegio de formar parte de la campaña de pruebas gratuitas por lo que no se cuenta con ingresos, pero si con la oportunidad de hacer pruebas reales y perfeccionar la aplicación. Incluye el soporte técnico para los clientes piloto, la implementación de ajustes según las observaciones recibidas y el monitoreo de métricas de uso y aceptación.
- Octava etapa: Documentación (Durante todo el año). Consiste en la redacción de manuales, guías de usuario y documentación técnica que respalde el uso de la aplicación. Se crearán documentos explicativos tanto para usuarios técnicos como no técnicos y elaborarán procedimientos para futuras actualizaciones.

4.5.3 Recursos Clave

Las necesidades para llevar a cabo este negocio giran en torno al consentimiento de gestión de datos del cliente y la posterior protección de estos datos.

El primer recurso clave es la creación de formularios que recojan el consentimiento de los clientes para procesar los datos, esto se consigue gracias a la opción de banners de cookies y gestión de privacidad en la herramienta onetrust. Con estos formularios se asegura el cumplimiento de consentimiento y transparencia estipulada en el GDPR.

El segundo recurso clave es la recolección de información sobre datos privados de los clientes que la aplicación recopila de los usuarios. Esto se puede realizar en el apartado de privacidad de onetrust y se asegura el cumplimiento de transparencia estipulada en el GDPR.

El segundo recurso consiste en la identificación y clasificación de datos sensibles. Esto se consigue gracias a Microsoft Purview que analiza tanto los datos introducidos en tiempo real desde su aplicación como los ficheros antiguos que había en la aplicación. Las empresas recopilan un gran número de datos y la identificación y clasificación manual puede ser tediosa. Para evitar esto se ofrecen servicios que usan sensores de clasificación automática, que detectan tipos de información confidencial preconfigurados (como nombres, direcciones, números de identificación) o permite configurar etiquetas personalizadas para encontrar datos en el sistema específicos de la empresa.

El tercer recurso consiste en la monitorización constante. Gracias a la clasificación realizada anteriormente, Microsoft Purview permite en su panel de actividades un seguimiento de datos tanto genérico como por su nivel de sensibilidad para un acceso más rápido y evitar la pérdida o dificultades de acceso dentro de la empresa de estos datos.

El cuarto recurso consiste en la prevención de pérdida de datos con la herramienta Data Loss Prevention en Microsoft Purview. Esta tecnología permite crear alertas o incluso bloquear acciones en las que se detecte que datos sensibles se envíen a externos o sean accedidos por personas no acreditadas.

El quinto recurso consiste en el cifrado ofrecido por Microsoft Purview cuando clasifica datos. Esta herramienta no solo identifica y aplica políticas de cifrado

a datos sensibles en reposo y en tránsito cuando se clasifican datos como se ha explicado en el segundo recurso. También administra claves de cifrado a través de Azure Key Vault para los datos. Azure Key Vault es un servicio de administración de claves para cifrar datos de aplicaciones y servicios que administra claves criptográficas, secretos y certificados digitales, genera y controla claves de cifrado utilizadas para proteger datos sensibles. Además, en todo momento monitoriza la conformidad con normativas como GDPR y otras que exigen cifrado.

5 Situación económica

En este apartado se abordará la situación económica del proyecto, que comprende el análisis de los aspectos financieros clave que influyen en su viabilidad y sostenibilidad.

5.1 Situación económica al inicio

En este apartado se recapitularán todos los recursos necesarios que se han comentado para poder calcular la financiación a realizar para el diseño de esta aplicación.

5.1.1 Inversión

En primer lugar, es importante resaltar que esta aplicación busca minimizar los costes. Esto se logra mediante la adopción de servicios en la nube de Microsoft Azure, como Microsoft Purview y otros servicios complementarios. Estas tecnologías minimizan los costes fijos para las empresas que buscan gestionar y proteger sus datos al no necesitar un hardware físico particular, con los gastos de mantenimiento asociados ni está limitado a una demanda concreta. La eliminación de la compra de hardware físico se debe a que no es necesario adquirir servidores, dispositivos de almacenamiento o equipos especializados, solo servicios software en la nube. La reducción de los costes de mantenimiento se debe a que, con Azure, Microsoft se encarga del mantenimiento del hardware, actualizaciones y parches de seguridad, liberando a las empresas de estos gastos recurrentes. La escalabilidad bajo demanda se refiere a que las empresas pueden aumentar o reducir la capacidad en función de sus necesidades, pagando únicamente por los recursos que realmente utilizan. La aplicación se encarga de buscar la combinación más económica de estos servicios, la aplicación de plantillas preestablecidas para algunas funcionalidades y un servicio de soporte.

No obstante, no todos los costes son variables. Para el correcto funcionamiento de la aplicación se requiere de personal que asista a las empresas, personal que vigile el funcionamiento de la aplicación y un gasto inicial en la creación de las plantillas y aplicación.

Presupuesto para el lanzamiento

A continuación, se explican los costes de los pasos a seguir para poder iniciar la actividad económica. Este presupuesto es de un año, el tiempo establecido para el lanzamiento en el apartado de actividades clave. Los gastos fijos serán estos más los sueldos de los socios iniciales. Estos empleados serán tres, que se encargarán de llevar a cabo el proceso y documentarlo hasta el lanzamiento. Una vez puesta en marcha serán los encargados de dar visibilidad y soporte a la aplicación. Las etapas del proyecto están detalladas en la figura 9, en el apartado de actividades clave. Con esta información se calculan sus respectivos castos fijos serán las siguientes:

Primero se prepararán los formularios que cumplan con la normativa GDPR, incluyendo validaciones automáticas, plantillas de consentimiento explícito y formularios de Evaluación de impacto (DPIA). Estos se realizarán para onetrust y se documentará el proceso necesario a seguir para llevar la adaptación a cada empresa. Por ello se necesitará para la implementación en onetrust que dos empleados ya con experiencia especialicen en la herramienta, esta plataforma ofrece certificaciones gratuitas y con entornos de prueba gratuitos. Por otra parte, una vez realizadas las plantillas se llevarán a una asesoría legal para confirmar el cumplimiento de la normativa.

- Para la formación y creación de plantillas se estima un plazo de dos meses, con un gasto está asociado de 3.400€ como bonus en formación.
- Para la asesoría legal se busca una asesoría online en servicios especializados como legalveritas que ofrecen también certificación de cumplimiento y se estima el gasto asociado en 250€

Formularios y Asesoría Legal	Costo (€)
Bonus en formación	3,400€
Asesoría legal (LegalVeritas)	250€
Total	3,650€

Tabla 2: Tabla de gastos de Formularios y Asesoría Legal

En segundo lugar, se prepararán guías para la clasificación de datos con herramientas de Microsoft, Esto supone un gasto en tasas de uso de la herramienta y otro en asesoría legal sobre el almacenamiento de datos para verificar el cumplimiento de la legislación.

- Coste de la herramienta: 1178€ mensuales [Anexo]
- Coste asesoría en legalveritas: 190€

Guías y Herramientas	Costo (€)
Herramienta Microsoft (10 meses)	11,780€
Suscripción Onetrust (10 meses)	10,000€
Asesoría legal (LegalVeritas)	190€
Total	21,970€

Tabla 3: Tabla de gastos de Guías y Herramientas

En tercer lugar, se preparará la estrategia de comercialización. Esto supone los gastos en la campaña digital, publicidad en redes sociales y Google Ads, gastos en la campaña presencial, participación en eventos y congresos y un presupuesto base para las pruebas gratuitas. Teniendo esto en cuenta el desglose sería el siguiente:

- Anuncios patrocinados en LinkedIn: €500 al mes (segmentación avanzada).
- Campañas visuales en Facebook e Instagram: €300 al mes (contenido multimedia atractivo).
- Creación de contenido visual y técnico: Contratación de un diseñador gráfico y un copywriter freelance: 1.500€ inicial para una biblioteca básica de contenido.

- Google Display Ads: Costo por clic (CPC): €0.50 (estimado), por tanto, para la campaña inicial mensual: €300.
- Participación en South Summit (Madrid): €1,500 (stand básico).
- Stand en DES (Digital Enterprise Show): €3,000 (paquete básico).
- Viajes y alojamiento: €1,000.
- Patrocinio en Foro de Ciberseguridad de CEOE: €2,500.
- Material promocional: €500.
- Suscripción mensual a onetrust:
- Suscripción mensual en Microsoft para cubrir aproximadamente 20 empresas

Estrategia de Comercialización	Costo (€)
Gastos iniciales:	
Creación de contenido (diseñador/copywriter)	1,500€
Gastos mensuales (6 meses):	
Anuncios patrocinados en LinkedIn	3,000€
Campañas en Facebook e Instagram	1,800€
Google Display Ads	1,800€
Costos únicos de eventos:	
South Summit	1,500€
Stand en DES	3,000€
Viajes y alojamiento	1,000€
Patrocinio Foro de Ciberseguridad CEOE	2,500€
Material promocional	500€
Total	16,600€

Tabla 4: Tabla de gastos de la Estrategia de Comercialización

En cuarto lugar, para personal se contará con tres empleados encargados de documentación, asistencia y supervisión, si se calcula un salario promedio de 35.000€ anuales, el costo total anual son 105.000€. No obstante, en los gastos también se debe incluir las cotizaciones a cargo de la empresa como son las contingencias comunes, accidentes de trabajo y enfermedades profesionales y el mecanismo de equidad intergeneracional, lo que supone un gasto aproximadamente del 32%. Por tanto, en total, el gasto por sueldos es de 138.600€. (SegurdidadSocial, 2024).

Sueldos	Costo Total (€)
Salario	138.600€
Seguridad Social (32%)	33.600€
Total	138.600€

Tabla 5: Tabla de gastos de sueldos de tres empleados

En quinto lugar, para posibles incidentes se va a crear una reserva para imprevistos. Esto es importante para cubrir posibles gastos que no hayan sido

contemplados. Esta aplicación es un nuevo proyecto, lo que conlleva un alto nivel de incertidumbre y pueden surgir gastos con los que no se contaba de forma original. En este caso se establecerá la reserva de un 10% de los gastos totales.

Teniendo todo esto en cuenta se presentan los siguientes gastos para el plan de lanzamiento, con una duración de un año. La duración de cada servicio en la tabla se indica en el diagrama de Gantt con planificación de las tareas de lanzamiento, en la figura 9, y se refleja en las tablas 2,3,4 y 5 dónde se encuentra el desglose de cada fila de gastos.

Suma de gastos	Costo Total (€)
Formularios y Asesoría Legal (desglose en la tabla 2)	3,400€
Guías y Herramientas (desglose en la tabla 3)	21,970€
Estrategia de Comercialización (desglose en la tabla 4)	16,600€
Sueldos (desglose en la tabla 5)	138.600€
Total gastos	180,820€
Reserva para incidentes	18,082
Total	198,902€

Tabla 6: Tabla de gastos totales

El presupuesto del lanzamiento de "Tecnologías ProtecciónData" está dividido en varias etapas clave: desarrollo de formularios y guías, herramientas, estrategia de comercialización y sueldos. Los gastos directos asociados a formaciones, formularios y guías ascienden a 3,400€, los de guías y licencias de software a 21,970€ y los de campañas de marketing digital y presencial a 16,600€. Además, los salarios de los tres empleados, encargados de la ejecución del proceso, suman un costo total de 180,820€durante el período de lanzamiento. La suma de todos los gastos calculados es de 180,820€, no obstante, se quiere dejar una reserva para incidencias del 10%, es decir de 18,000€. En conjunto, la inversión total para esta fase es de 198,902€.

5.1.2 Financiación

Las fuentes de financiación que se contemplan son las propias y ajenas. Las fuentes de financiación propia son los recursos monetarios aportados por los propietarios de la empresa y no han sido repartidos, más los aportados por terceros sin exigencia de devolución. La principal ventaja que tiene es la libertad de acción que ofrece, la solvencia financiera y por tanto la autonomía que denota la empresa. Por otra parte, las fuentes de financiación ajenas son aquellos que han sido cedidos por terceros a la empresa de forma temporal con la exigencia devolución con o sin intereses en una determinada fecha. Las ventajas de estos fondos son el incremento de rentabilidad a los activos de capital propio, creando un efecto expansivo y un posible efecto apalancamiento, por otro lado, como desventaja tiene el efecto endeudamiento y necesidad de solvencia para compensar los pagos. (María de los Angeles Gil Estallo, 2007). En la figura 10 se muestra la distribución de la financiación que se busca como objetivo.

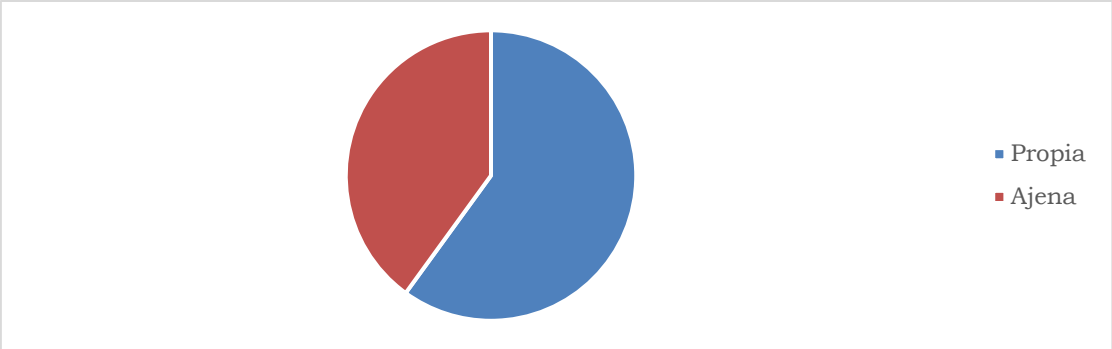

Figura 10: Distribución de la financiación

Los fondos propios deben ser suficientes para garantizar solvencia. Por ello, la estrategia de financiación consistirá en buscar en 40% de fondos propios y el 60% de fondos ajenos.

Para la financiación ajena se optará por un préstamo bancario a dos años, ya que es en el segundo año cuando se espera tener beneficio. Un préstamo te permite financiar un porcentaje significativo del costo total de la empresa, recibiendo la totalidad del importe desde el primer momento. Este dinero será reembolsado con intereses a lo largo del tiempo. Esto permite tener todo el capital necesario de inmediato. Este préstamo será del 60% de los gastos de lanzamiento y del 60% de los gastos previstos para los dos años siguientes como se puede ver en la figura x. Los gastos previstos para la inversión del año 0 sin tener en cuenta los intereses y primeros pagos del préstamo son 198,902€. Si se quiere financiar un 60% de este gasto con un préstamo es necesario pedir 119.341€ para este año y 118.357€ para futuros años (60% de 198,627€, el gasto calculado en la tabla 7). Este préstamo comenzará en el sexto mes del año 0, ya que los primeros meses no requieren de tanta financiación. Además, se añadirá una cláusula por la cual los pagos de capital de los primeros seis meses se pagarán acumulados al año desde el inicio del préstamo ya que es en esta fecha en la que comienzan las ventas. De esta forma se pagan los intereses desde el inicio, pero se cuenta con más tiempo para recaudar dinero de las ventas.

Para la financiación propia se busca financiar el 40% de los gastos totales, es decir 79.560€. No obstante, también se debe tener en cuenta que en ese mismo año aún sin ingresos se deben financiar 5.086€ de intereses del préstamo y parte del capital. Por ello, se exigirá una mayor cantidad de fondos propios, 90.000€ a desembolsar en el año 0. Para reembolsarlo se prevé que la empresa comenzará a generar beneficios a partir del segundo año de operaciones. Esto permitirá que la empresa cubra los pagos del préstamo sin afectar su liquidez ni poner en riesgo su estabilidad financiera.

Más adelante, cuando el lanzamiento de la aplicación se haya puesto en marcha se recurrirá a subvenciones de la Unión Europea y a ingresos de las ventas del servicio. Todos estos detalles se incluyen en el siguiente capítulo del proyecto.

5.2 Situación económica durante el proyecto

En este apartado se analizarán las previsiones de situación económica del proyecto tras su lanzamiento.

5.2.1 Gastos

Una vez pasado el periodo de lanzamiento los gastos de la aplicación consistirán en el pago de las herramientas utilizadas, una auditoria por trimestre para asegurar el cumplimiento de la normativa, sueldos y la campaña publicitaria.

Suma de gastos	Costo Total (€)
Guías y Herramientas	21,970€
Estrategia de Comercialización	16,600€
Sueldos	138,600€
Asesoramiento legal	3,400€
Gasto total	180,570€
Reserva para imprevistos	18,057€
Total	198,627€

Tabla 7: Gastos durante el proyecto

Estos son los gastos que se prevén. No obstante, no todos ellos son fijos. Tanto el gasto en herramientas como en asesoría legal aumentará según el número de clientes crece y se requieren más servicios. Para una mayor precisión se calcularán los flujos de caja y la cuenta de pérdidas y ganancias con un mayor detalle.

5.2.1.1 Cuadros de amortizaciones

Para poder saber los gastos asociados a cada préstamo se han realizado los cuadros de amortizaciones. Un cuadro de amortización es una tabla detallada que muestra cómo se distribuyen los pagos de un préstamo durante su plazo. Permite ver, para cada cuota, cómo se desglosan los pagos entre: Capital, la parte del pago que reduce el saldo pendiente del préstamo; intereses, la parte del pago que se destina a cubrir el costo del préstamo (calculado sobre el saldo restante); saldo pendiente, la cantidad que aún queda por devolver después de realizar el pago. Para poder tener unos valores iniciales, se han realizado las estimaciones del simulador de préstamos del Banco Santander para un préstamo de 60.000 euros, se calculan las condiciones de los préstamos necesarios para el año 0 y para el año 1, ambos préstamos serán a dos años para tener un plazo superior de pago de intereses en caso de necesidad.

Préstamo del año 0

No.	Cuota	Capital	Intereses	Saldo
0				119.341,00 €
1	5.259,74 €	4.717,73 €	542,007042	114.623,27 €
2	5.259,74 €	4.739,16 €	520,580673	109.884,11 €
3	5.259,74 €	4.760,68 €	499,056993	105.123,43 €
4	5.259,74 €	4.782,30 €	477,435559	100.341,12 €
5	5.259,74 €	4.804,02 €	455,715929	95.537,10 €
6	5.259,74 €	4.825,84 €	433,897655	90.711,26 €

7	5.259,74 €	4.847,76 €	411,980289	85.863,50 €
8	5.259,74 €	4.869,78 €	389,963382	80.993,72 €
9	5.259,74 €	4.891,89 €	367,846482	76.101,83 €
10	5.259,74 €	4.914,11 €	345,629134	71.187,72 €
11	5.259,74 €	4.936,43 €	323,310882	66.251,29 €
12	5.259,74 €	4.958,85 €	300,891269	61.292,44 €
13	5.259,74 €	4.981,37 €	278,369833	56.311,07 €
14	5.259,74 €	5.003,99 €	255,746112	51.307,08 €
15	5.259,74 €	5.026,72 €	233,019641	46.280,36 €
16	5.259,74 €	5.049,55 €	210,189955	41.230,81 €
17	5.259,74 €	5.072,48 €	187,256584	36.158,32 €
18	5.259,74 €	5.095,52 €	164,219057	31.062,80 €
19	5.259,74 €	5.118,66 €	141,076901	25.944,14 €
20	5.259,74 €	5.141,91 €	117,829641	20.802,23 €
21	5.259,74 €	5.165,26 €	94,4768001	15.636,97 €
22	5.259,74 €	5.188,72 €	71,0178983	10.448,25 €
23	5.259,74 €	5.212,29 €	47,452454	5.235,96 €
24	5.259,74 €	5.235,96 €	23,7799832	-0,00 €

Tabla 8: Cuadro de amortizaciones del préstamo del año 0

Cada cuota fija de 5,259.74 € se descompone en una parte destinada al pago del capital y otra a los intereses, los cuales disminuyen progresivamente a medida que se reduce el saldo pendiente. Inicialmente, una mayor proporción de la cuota cubre los intereses (542.01 € en la primera cuota), pero con cada pago, la proporción destinada al capital aumenta de 4,717.73 € en la primera cuota a 5,235.96 € en la última. Esto permite calcular los pagos en cada año.

Por tanto, si se tiene en cuenta que el préstamo empieza en el sexto mes del año 0:

Intereses año 0	2.928,69 €
Intereses año 1	3.468,42 €
Intereses año 2	495,63 €

Capital año 0	28.629,74 €
Capital año 1	59.648,45 €
Capital año 2	31.062,80 €

Tabla 9:Intereses y capital a pagar préstamo del año 0

Una vez diferenciados los pagos del préstamo a realizar en cada año es posible realizar las cuentas anuales.

Préstamo del año 1 y 2

No.	Cuota	Capital	Intereses	Saldo
0				118.357,00 €
1	5.216,37 €	4.678,83 €	537,538042	113.678,17 €
2	5.216,37 €	4.700,08 €	516,288339	108.978,08 €

3	5.216,37 €	4.721,43 €	494,942128	104.256,65 €
4	5.216,37 €	4.742,87 €	473,498969	99.513,78 €
5	5.216,37 €	4.764,41 €	451,958423	94.749,37 €
6	5.216,37 €	4.786,05 €	430,320047	89.963,32 €
7	5.216,37 €	4.807,79 €	408,583396	85.155,53 €
8	5.216,37 €	4.829,62 €	386,748025	80.325,90 €
9	5.216,37 €	4.851,56 €	364,813485	75.474,35 €
10	5.216,37 €	4.873,59 €	342,779325	70.600,75 €
11	5.216,37 €	4.895,73 €	320,645094	65.705,03 €
12	5.216,37 €	4.917,96 €	298,410336	60.787,07 €
13	5.216,37 €	4.940,30 €	276,074595	55.846,77 €
14	5.216,37 €	4.962,73 €	253,637413	50.884,04 €
15	5.216,37 €	4.985,27 €	231,098329	45.898,76 €
16	5.216,37 €	5.007,91 €	208,45688	40.890,85 €
17	5.216,37 €	5.030,66 €	185,712601	35.860,19 €
18	5.216,37 €	5.053,51 €	162,865024	30.806,68 €
19	5.216,37 €	5.076,46 €	139,913682	25.730,22 €
20	5.216,37 €	5.099,51 €	116,858103	20.630,71 €
21	5.216,37 €	5.122,67 €	93,6978124	15.508,04 €
22	5.216,37 €	5.145,94 €	70,4323358	10.362,10 €
23	5.216,37 €	5.169,31 €	47,0611952	5.192,79 €
24	5.216,37 €	5.192,79 €	23,5839106	-0,00 €

Tabla 10: Cuadro de amortizaciones del préstamo del año 1

Cada cuota fija de 5.216,37 € se descompone en una parte destinada al pago del capital y otra a los intereses, los cuales disminuyen progresivamente a medida que se reduce el saldo pendiente. Inicialmente, una mayor proporción de la cuota cubre los intereses (537,53 € en la primera cuota), pero con cada pago, la proporción destinada al capital aumenta de 4.678,83 € en la primera cuota a 5.192,79€ en la última. Esto permite calcular los pagos en cada año.

Por tanto:

Intereses año 1	5.026,53 €
Intereses año 2	1.809,39 €

Capital año 1	57.569,93 €
Capital año 2	60.787,07 €

Tabla 11::Intereses y capital a pagar préstamo del año 1

Ahora que están establecidos y desglosados los pagos a realizar se puede calcular el total a pagar por los préstamos:

Año 0:

- Intereses: 2.928,69 €
- Capital: 28.629,74 € (se pagará por cláusula en el año 1)

Año 1:

- Intereses: 3.468,42 € + 5.026,53 € = 8.494,42 €
- Capital sin acumulado año 0: 59.648,45 €+ 57.569,93 € = 118862,35 €
- Capital con acumulado año 0: 118.862,35 €+28.629,74 €= 145.848,13 €

Año 2:

- Intereses: 495,63 €+1.809,39 € =2.305,02 €
- Capital: 31.062,80 €+60.787,07 € = 91.849,80 €

En la siguiente tabla se observan los flujos financieros que se esperan para los primeros tres años en los que se espera recibir y pagar este préstamo.

Concepto	Año 0	Año 1	Año 2
Salidas año anterior		116,412	80,427
Entradas			
Préstamos	119,341	118,357	
Total Entradas	119,341	234,769	80,427
Salidas			
Intereses del préstamo	-2,929	-8,494	-2,305
Pagos del préstamo		-145,848	-91,849
Total Salidas	-2,929	-154,342	-94,154
Flujo Neto	116,412	80,427	-13,727

Tabla 12: Flujos del préstamo los tres primeros años.

Este préstamo tiene como objetivo ofrecer liquidez en los primeros años de inversión en la aplicación, el resultado final es una pérdida de 13,727mil euros en el segundo año aportando una mejor solvencia durante los dos primeros para conseguir compensar las pérdidas de los flujos de caja mostrados en la tabla 16.

5.2.2 Ingresos

El proyecto cuenta con tres fuentes de financiación. En primer lugar, los recursos generados por el negocio, se espera que cada vez las ventas sean mayores y provienen de diferentes tipos de tarifas, cada una se espera que tenga un número de clientes proporcional a su complejidad, no obstante, esta fuente de ingresos comienza un año tras el inicio del proceso productivo. En segundo lugar, de préstamos bancarios, como es el caso de la inversión inicial. En tercer lugar, de aportaciones de los accionistas (recursos propios).

También se contempla a largo plazo la opción de ingresos por subvenciones, en los últimos años, la Unión Europea ha incrementado significativamente las subvenciones y fondos destinados a la innovación digital, con un enfoque particular en áreas clave como la ciberseguridad y la protección de datos. Esto responde a la creciente preocupación por la protección de la información y la necesidad de contar con infraestructuras digitales seguras en un entorno cada vez más interconectado. Iniciativas como el Programa Digital Europa y el Fondo Horizonte Europa reflejan este compromiso, proporcionando financiación a proyectos que busquen mejorar la resiliencia digital y asegurar el cumplimiento

normativo en el tratamiento de datos. En este contexto, la aplicación, que ofrece soluciones para garantizar la privacidad y seguridad de los datos en cumplimiento con el Reglamento General de Protección de Datos (GDPR) en pequeñas y medianas empresas españolas, se beneficia directamente de estas subvenciones. Se alinea con los objetivos de la UE en cuanto a la mejora de la ciberseguridad y la protección de datos personales, especialmente aquellas empresas con dificultades para acceder a estos recursos. En concreto, los programas de EIC Accelerator (634 millones de euros) y EIC Strategic Technologies for Europe Platform (STEP) Scale Up (300 millones de euros)

El EIC Accelerator está destinado a startups y pymes que desarrollen y escalen innovaciones con el potencial de crear nuevos mercados o de disrumpir los existentes. Este programa está especialmente enfocado en innovaciones disruptivas y en empresas que busquen un alto impacto económico y social. Específicamente, dirigido a startups tecnológicas, pymes innovadoras y empresas con un gran potencial de crecimiento en sectores como la inteligencia artificial, la ciberseguridad, las tecnologías limpias, etc. También para proyectos con innovaciones que pueden tener un impacto global o transformar sectores industriales. Se busca escalar soluciones que ya estén validadas, pero que necesitan apoyo para la expansión. Este programa ofrece subvenciones de hasta 2.5 millones de euros para apoyar el desarrollo y escalado del proyecto, junto con inversiones de entre 0.5 a 10 millones de euros. Las inversiones pueden ser realizadas en forma de capital riesgo. Este programa encaja con nuestra aplicación, que actualmente cuenta con únicamente tres socios, ofrece una solución tecnológica a problemas de seguridad de datos y aporta un valor social al ser su público objetivo pequeñas y medianas empresas con menos recursos.

Si se decide que la empresa se lleva a gran escala, atendiendo a PYMES no solo españolas sino de toda Europa, se puede recurrir a EIC Strategic Technologies for Europe Platform (STEP) Scale Up (300 millones de euros) es un esquema busca proporcionar financiación adicional en forma de capital para startups, pymes, spin-offs y pequeñas medianas empresas (small mid-caps) que estén innovando en áreas estratégicas clave para la UE. El foco está en empresas que ya están en una fase avanzada de innovación, pero que necesitan cofinanciación privada para continuar su expansión. Está dirigido a empresas tecnológicas que estén trabajando en áreas críticas como la energía renovable, la tecnología médica, la ciberseguridad, la inteligencia artificial, entre otros. Este esquema proporciona inversiones de entre 10 y 30 millones de euros, con el objetivo de atraer cofinanciación privada para asegurar que las empresas puedan seguir escalando. (EuropeanInnovationCouncil, 2024)

En cuanto a la opción de financiación mediante las ventas del servicio requiere una estrategia de establecimiento de precios. Es importante recordar que el objetivo de la aplicación es ofrecer recursos a un precio más asequible. Es por esto por lo que dependiendo del servicio solicitado se realizarán una serie de servicios y otros. De esta forma se garantiza que todas las empresas puedan cumplir el GDPR y disponer de más o menos servicios para proteger sus datos según su presupuesto. En la tabla 13 se indican los diferentes servicios y las correspondientes tarifas que se ofrecerán en la aplicación.

Servicio	Tarifa
Servicio mínimo	300€/mes
Servicio básico	500€/mes
Servicio experto	800€/mes

Servicio completo	1.220€/mes

Tabla 13: Rango de tarifas de precios de la aplicación

El servicio mínimo de recopilación de datos y consentimiento únicamente usa la herramienta onetrust y se encarga de la creación de banners de cookies, de consentimiento y de formularios DPIA además de la recolección segura de estos datos con el cifrado mínimo certificado por servicios de auditoría legal. No incluye servicios de clasificación de datos, cifrado experto, prevención de pérdidas o monitoreo. A nivel interno de gastos solo consume onetrust y no supone ninguna necesidad de Microsoft Purview.

El servicio básico incluye el servicio mínimo más la clasificación de datos y cifrado experto. No obstante, no incluye reglas para la prevención de pérdida de datos ni monitorización. A nivel interno consume servicios de onetrust y de Microsoft Purview, pero no de llamadas extra a APIs con coste añadido para la empresa

El servicio experto incluye el servicio básico más la inclusión de reglas de prevención de datos, es decir bloquea acciones peligrosas o envía alertas en situaciones de riesgo de pérdida de datos, pero no incluye la monitorización. A nivel interno usa tanto onetrust como servicios Microsoft Purview como llamas extra a APIs que nos suponen un coste extra pero no se necesita servicios DevOps de monitoreos constantes.

El servicio completo incluye el servicio experto más la monitorización y entrega de informes con la información de datos sensibles que posee la empresa y el rastreo y seguimiento continuo en tiempo real y archivos antiguos de los mismos. Este servicio usa todos los recursos que la aplicación dispone.

Ingresos por ventas

Se han establecido las tarifas, se pueden consultar en la tabla 8. Hay cuatro tipos de servicio en la aplicación. Se estima una distribución basada en la complejidad y demanda del servicio:

- Servicio mínimo: 40% de clientes
- Servicio básico: 30% de clientes
- Servicio experto: 20% de clientes
- Servicio completo: 10% de clientes

También se calcula que cada año el número de clientes se irá incrementando, se calcularán un total de 50 clientes el primer año y 60 el segundo año. No obstante, del primer año solo se tendrá en cuenta el 70% de los ingresos ya que parte de los meses corresponderán a pruebas gratuitas y algunos clientes se calculan desde enero cuando posiblemente su incorporación real sea más adelante. En el segundo año se seguirá esta misma estrategia, pero debido a que ya tienen algunos clientes fidelizados de tendrá en cuenta el 80% de los ingresos.

En la tabla 14 se puede observar las ventas previstas en el año 1 si todos los clientes fuesen anuales y sin tener en cuenta la prueba gratuita inicial, algunos si serán así ya que a finales del año 0 ya se contemplan pruebas a cliente, pero en posteriores cálculos del primer año solo se tendrá en cuenta el 70% por estos motivos.

Servicio	Clientes	Tarifa Mensual (€)	Ingresos Mensuales (€)	Ingresos Anuales (€)

Servicio mínimo	20	300	6,000	72,000
Servicio básico	15	500	7,500	90,000
Servicio experto	10	800	8,000	96,000
Servicio completo	5	1,220	6,100	73,200
Total	50	-	27,600	331,200

Tabla 14: Ventas previstas en el año 1

En la tabla 15 se puede observar las ventas previstas en el año 2 si todos los clientes fuesen anuales y sin tener en cuenta la prueba gratuita inicial, estos casos si serán menores ya que se contará con clientes de finales del año 0 y año 1, pero en posteriores cálculos del primer año solo se tendrá en cuenta el 80% por estos motivos.

Servicio	Clientes	Tarifa Mensual (€)	Ingresos Mensuales (€)	Ingresos Anuales (€)
Servicio mínimo	24	300	7,200	86,400
Servicio básico	18	500	9,000	108,000
Servicio experto	12	800	9,600	115,200
Servicio completo	6	1,220	7,320	87,840
Total	60	-	33,120	397,440

Tabla 15:Ventas previstas en el año 2

En las tablas 14 y 15 de ventas anuales se muestra el ingreso que se obtendría si todos los clientes demandasen un servicio todos los meses del año, en el primer año se espera que el ingreso sea de un 70% de este total y en el año dos de un 80%, ya que no todos los clientes se fidelizarán desde el primer momento del año. En la tabla 16 se muestran los ingresos totales por ventas.

Año del ingreso	Cantidad (miles de euros)
Año 1: 70% de 331,200	231,84
Año 2: 80% de 397,440	317,95

Tabla 16: Ingresos por ventas en los años 1 y 2

Por tanto, los ingresos para los primeros años son obtenidos por ventas de diferentes servicios en la aplicación, las cuales se espera que crezcan los primeros años.

5.2.3 Flujos de caja (previstos)

Los flujos de caja son un análisis financiero que muestra las entradas y salidas de efectivo en un periodo determinado, permiten evaluar la capacidad de la empresa para generar efectivo y cumplir con sus obligaciones financieras.

Incluyen las fuentes de ingresos (ventas, préstamos, subvenciones, etc.) y los desembolsos asociados (sueldos, intereses, pagos de préstamos, entre otros). Estos flujos de caja se representan en la tabla 17 para los cinco primeros años de la inversión.

Concepto	Año 0	Año 1	Año 2	Año 3	Año 4
Saldo año anterior		-108,570	-76,000	42,430	160,860
Entradas de efectivo					
Fondos propios	90				
Ventas del servicio	0	231,84	317,95	317,95	317,950
Total Entradas	90	231,84	317,95	317,95	317,950
Salidas de efectivo				0	0,000
Sueldos (contado SS)	-138,6	-138,6	-138,6	-138,6	-138,600
Herramientas (Microsoft/Onetrust)	-21,97	-23,97	-25,97	-25,97	-25,970
Campañas de marketing	-16,6	-14,6	-12,6	-12,6	-12,600
Asesoría legal	-3,4	-4	-4,25	-4,25	-4,250
Reserva para imprevistos	-18	-18,1	-18,1	-18,1	-18,100
Total Salidas	-198,570	-199,27	-199,52	-199,52	-199,520
Flujo Neto	-108,570	-76,000	42,430	160,860	279,290

Tabla 17: Flujos de caja (miles de euros) previstos de los cinco primeros años

En los flujos de caja previstos, se observa que, en el año 0, las entradas únicamente son inversiones de fondos propios (90mil €), por lo que las salidas superan las entradas, resultando en un flujo neto negativo de -108,570€ que serán una entrada en los siguientes años. En el Año 1, el flujo neto mejora con un inicio en ventas (231,84mil€) reduciendo las pérdidas en el resultado neto (-76,000mil €), aun con un flujo negativo. En el año 2, la tendencia continúa mejorando con ventas en crecimiento (317,95mil €) y un flujo neto que comienza a ser positivo (42,430mil€), mostrando que el modelo de negocio comienza a generar un exceso de liquidez y sostenibilidad a medida que madura. En el año 3 y 4 se prevén los mismos ingresos por ventas que en el año 2, ya que la aplicación ya estaría asentada, se aprecia un aumento del flujo neto en estos años.

Cuadro de financiación

Una vez obtenidos los flujos de caja se debe tener en cuenta que una de las fuentes de financiación son los préstamos bancarios no contemplados en estas

cuentas. En la tabla 12 se observan los flujos de estos préstamos en los tres primeros años, cuyo fin es dar solvencia durante los años de lanzamiento, los cuales son negativos de acuerdo a la tabla de flujos de caja. Para poder observar cual es la fuente de financiación de gastos durante cada año se muestra en la tabla 18 el cuadro de financiación con todas las fuentes.

Concepto	Año 0	Año 1	Año 2
Flujo Operativo	-108,57	-76	42,43
Flujo Financiero	116,412	80,427	-13,727
Total	7,842	4,427	28,703

Tabla 18: Cuadro de financiación en miles de euros

Estos préstamos permiten mantener la solvencia mientras se consolida la actividad operativa, la cual comienza a generar flujos positivos en el año 2. El cuadro de financiación proporciona una visión de cómo se equilibran las fuentes de financiación en cada etapa, asegurando la viabilidad del proyecto a corto y medio plazo.

5.2.4 Cuenta de pérdidas y ganancias

La cuenta de pérdidas y ganancias es un estado financiero que muestra el rendimiento económico de una empresa durante un período específico, detallando los ingresos generados, los costos asociados a la operación, y los resultados finales. Incluye los ingresos (como ventas y subvenciones), los costos directos (relacionados directamente con la prestación del servicio o producto), los costos financieros (como intereses de préstamos), y los gastos operativos, para llegar al resultado neto, que puede ser una ganancia o pérdida. La cuenta prevista para los tres primeros años de la aplicación se muestra en la tabla 18.

Concepto	Año 0	Año 1	Año 2
Ingresos			
Ventas del servicio	0	231,84	317,95
Total Ingresos	0	231,84	317,95
Costos Directos			
Sueldos	-138,6	-138,6	-138,6
Herramientas (Microsoft/Onetrust)	-21,97	-23,97	-25,97
Campañas de marketing	-16,6	-16,6	-16,6
Formularios y Asesoría legal	-3,4	-4	-4,25
Total Costos Directos	-180,57	-183,17	-185,42
Costos Financieros			
Intereses del préstamo	0,000	-8,494	-2,305
Total Costos Financieros	0	-8,494	-2,305
Resultado Operativo	-180,57	40,176	130,225
Reserva para imprevistos	-18	-18,1	-18,1
Resultado Neto	-198,57	22,076	112,125

Tabla 19: Cuenta de pérdidas y ganancias prevista en los tres primeros años

En esta proyección, el año 0 muestra una situación inicial sin ingresos, ya que aún no se han iniciado las ventas y altos costos operativos, financieros, y directos. Esto lleva a un resultado neto negativo (-198,57 mil€), propio de una etapa de inicio con fuertes inversiones y escasos ingresos.

En el año 1, comienzan los ingresos por ventas (231,84mil€) impulsada por las ventas del servicio. Sin embargo, los costos financieros aumentan considerablemente debido a los pagos del préstamo inicial y el segundo préstamo. Gracias a ello, el resultado es positivo, 22,076 mil €, hay mejores resultados que el año anterior, mostrando un progreso hacia el equilibrio.

En el año 2, el negocio continua mejorando, con ingresos mayores (317,95mil €) sin necesidad de recurrir a préstamos bancarios, resultado del crecimiento en ventas y subvenciones. Aunque los costos financieros y operativos se mantienen altos, el resultado neto positivo (112,125 mil €) refleja que la empresa ha alcanzado sostenibilidad financiera, marcando el inicio de la recuperación de la inversión inicial y consolidación del modelo de negocio.

De esta forma se espera una mejoría económica en los siguientes años donde ya no se prevé

5.2.5 Índices de rentabilidad

En esta sección se aplicarán algunos índices de rentabilidad financiera e indicadores que ayuden a evaluar financieramente la aplicación.

Costo de Capital Promedio Ponderado (WACC)

Es el costo promedio ponderado de capital, que representa el costo que tiene una empresa para financiarse combinando deuda y capital propio. Se utiliza para valorar inversiones, ya que es la tasa mínima de retorno que un proyecto debe generar para ser rentable. La fórmula para calcularlo es la siguiente:

$$\text{WACC} = \left(\frac{E}{V} \times Re\right) + \left(\frac{D}{V} \times Rd \times (1 - Tc)\right)$$

Donde:

- E=Valor de mercado del capital de la empresa
- D=Valor de mercado de la deuda de la empresa
- V=E+D
- Re=Costo del capital
- Rd=Costo de la deuda
- Tc=Tasa del impuesto corporativo

Para calcularlo en la aplicación se usarán los siguientes valores:

- Capital propio (E): 90.000€ aportados en la inversión inicial.
- Deuda (D): 60% de la inversión inicial de, es decir: D=198.902×0.6=119.341,2
- Costo del capital propio (Re): Se calcula que los accionistas esperan un retorno del 15%.
- Costo de la deuda (Rd): El interés del préstamo es 5.45%.

- Tasa impositiva (TT): Se calcula una tasa de impuestos del 25% ya que, en España, el Impuesto de Sociedades es la tasa más común y es del 25% para la mayoría de las empresas

$$WACC = \left(\frac{90.000}{209341,2} x 15\%\right) + \left(\frac{119.341,2}{209341,2}\ x\ 5,45\%\ x\ (1 - 25\%)\right)$$

WACC = 8,78%

Esto significa que, por cada euro invertido en el proyecto, la empresa necesita obtener un retorno de al menos 8,78% para cubrir el costo de sus fuentes de financiamiento (capital propio y deuda).

(Hargrave, 2024)

VAN (Valor Actual Neto)

VAN (Valor Actual Neto) o Net Present Value (NPV) es el valor presente de los flujos de caja futuros generados por un proyecto, mide la rentabilidad absoluta de una inversión. Un VAN positivo indica que el proyecto generará valor. La fórmula es la siguiente:

$$NPV_{XYZ} = \frac{Z_1}{1+r} + \frac{Z_2}{(1+r)^2} - X_0$$

Y los valores significan:

- Z1 = Flujo de caja en el tiempo 1
- Z2 = Flujo de caja en el tiempo 2
- r = tasa de descuento; en este caso se usará el WACC
- X0 = Salida de efectivo en el tiempo 0 (es decir, el precio de compra/inversión inicial)

Para calcularlo, se ha usado la fórmula de Excel VNA teniendo en cuenta los flujos de efectivo calculados con anterioridad, la inversión inicial y el WACC. El resultado es de VAN= 167,185€, lo que indica que la inversión generará más ingresos de los que se invirtieron inicialmente, descontados a su valor presente. Es decir, la inversión es rentable y se espera que agregue valor a la empresa o al inversor. Este Excel se encuentra en el anexo III

(CorporateFinanceInstitute)

TIR (Tasa Interna de Retorno)

Es la tasa de descuento que hace que el VAN de un proyecto sea igual a cero. Mide la rentabilidad relativa de una inversión y se compara con la tasa mínima aceptable. La fórmula es la siguiente:

$$0 = CF_0 + \frac{CF_1}{(1+IRR)} + \frac{CF_2}{(1+IRR)^2} + \frac{CF_3}{(1+IRR)^3} + \ldots + \frac{CF_n}{(1+IRR)^n}$$

Or

$$0 = NPV = \sum_{n=0}^{N} \frac{CF_n}{(1+IRR)^n}$$

Y los valores significan:

- CF0= Inversión inicial
- CF1, CF2, CF3… = Flujos de caja
- N = Cada periodo
- N = el periodo actual
- NPV= Valor Neto Presente
- IRR = Tasa Interna de Retorno

Para resolverlo aplicado al proyecto se calcula con la fórmula de Excel. Se tienen en cuenta los flujos de caja de la tabla 15. Por tanto, el TIR es del 37%, lo que indica una alta rentabilidad. Especialmente es destacable comparada con el WACC del 8,78% generaría un retorno mucho mayor que el costo del capital de la empresa, lo que lo hace atractivo desde una perspectiva financiera.

(Vipong)

ROA (Rentabilidad sobre los Activos)

El ROA mide qué tan eficientemente una empresa utiliza sus activos totales para generar beneficios. Es un indicador de la capacidad de la empresa para utilizar su base de activos para generar ingresos netos. La fórmula es la siguiente:

$$\text{ROA} = \frac{\text{Beneficio neto}}{\text{Activos totales}} \times 100$$

Por tanto, aplicado a este proyecto, teniendo en cuenta la cuenta de pérdidas y ganancias prevista calculada anteriormente:

$$\text{ROA}_2 = \frac{28{,}703}{180{,}57} \times 100 = 15{,}89\%$$

En el segundo año cuando la empresa está siendo altamente eficiente en generar ganancias netas en relación con los costos directos, por cada 100 € de costos directos, la empresa ha generado 15,89 € de beneficios netos.

6 Resultados y conclusiones

La aplicación ofrece una solución a un problema claro al que se enfrentan las empresas hoy en día: la seguridad de datos. Las pequeñas y medianes empresas de todos los sectores recogen datos personales de empleados, clientes, proveedores e interesados. No todas las empresas tienen los recursos para recopilar los datos sensibles con los que cuentan y protegerlos, sin embargo, esta tarea es exigida por ley y compromete su seguridad.

La aplicación usa servicios principalmente de onetrust y Microsoft. Estos recursos comparten el ser servicios software, lo que implica que no se compra y contratan instalaciones o bienes con gastos fijos. Utiliza servicios en la nube que, al ser usados para diferentes empresas con los mismos recursos, minimiza los costes. Asegurando la seguridad en unos recursos compatibles para todas las empresas y distribuibles reduce los gastos sin repercusión a la calidad del servicio.

Desde el punto de vista normativo, esta aplicación tiene un impacto social notable. Actualmente, las empresas con menos recursos enfrentan dificultades para cumplir con legislaciones complejas en materia tecnológica, lo que a menudo genera una brecha social entre grandes corporaciones y pequeñas empresas. La aplicación busca cerrar esta brecha ofreciendo herramientas asequibles y accesibles, contribuyendo a una mayor equidad en el acceso a tecnologías críticas. Al ser una herramienta basada en la nube, no solo reduce costos, sino que también garantiza una rápida adaptación a las normativas específicas de cada región, lo que la hace escalable.

El plan de negocio cuenta con propuestas para penetrar en el sector tecnológico, con un alto nivel de competencia y en el que es difícil crear una imagen de calidad. Las distintas estrategias de marketing propuestas, especialmente el posibilitar pruebas gratuitas en un límite de tiempo permite mostrar la calidad y atraer a más clientes.

Una de las principales barreras a las que se enfrentan hoy en día las empresas con menos recursos es el cumplimiento de la legislación en ámbitos tecnológicos. Esta normativa requiere de formación y conocimiento tanto para entenderla como para llevarla a cabo. Es impuesta en todos los sectores por necesidad de una mayor seguridad y crea una brecha social que esta aplicación busca solventar.

Además, una conclusión a destacar es como los valores de la aplicación se alinean con los de los objetivos de la unión europea que buscan eliminar brechas tecnológicas como la que se crea en seguridad de datos. Esta similitud hace que opte a subvenciones europeas que buscan el avance tecnológico, la protección en el mundo digital y la integración social.

Desde una perspectiva financiera, los cálculos realizados del WACC, VAN, TIR y ROA confirman la rentabilidad del proyecto a medio plazo. Requiere una inversión de 90.000€ por parte de los accionistas y el resto se financia mediante préstamos bancarios de forma inicial. Se debe tener en cuenta que la propuesta tiene como objetivo ser solvente a los dos años, es en este segundo año cuando se devuelven todos los préstamos obtenidos y se siguen manteniendo beneficios. En el segundo año se espera una ROA del 15,89%, por lo que en tan solo dos años ya es eficiente económicamente y se ha compensado la inversión inicial. Esto indica que la empresa está no solo en camino de recuperar la inversión, sino también de generar beneficios significativos a largo plazo. Además, un

Valor Actual Neto de 167,185 € muestra que la propuesta tiene un alto potencial de éxito financiero.
En términos de sostenibilidad, la aplicación no solo es eficiente en costos, sino que también contribuye a una reducción de la huella de carbono al emplear tecnologías en la nube en lugar de infraestructura física. Este enfoque, además, permite una integración ágil de nuevos usuarios y una mejora continua de los servicios ofrecidos.

Finalmente, cabe a destacar el potencial de expansión del proyecto. A futuro, se vislumbran estrategias de internacionalización, integración con plataformas tecnológicas complementarias y la posibilidad de diversificar los servicios para incluir nuevas funcionalidades adaptadas a sectores específicos. Además, al tener una visión alineada con la Unión Europea, hay una gran oportunidad de realizar colaboraciones estratégicas con instituciones académicas y gubernamentales que podrían fortalecer su impacto y garantizar su vigencia en un entorno tecnológico en constante evolución.

7 Análisis de Impacto

En este capítulo se analizará el impacto que la aplicación puede causar a nivel personal, empresarial, social, económico, medioambiental y cultural. Posteriormente también se relacionará este impacto con los Objetivos de Desarrollo Sostenible (ODS).

El plan de negocio está basado en el modelo Canvas Social, que busca acercarse a la posibilidad de general valor no sólo económico, sino también social y ambiental de la iniciativa de negocio que se quiere analizar.

La primera decisión tomada, y la más relevante para conseguir una mejora medioambiental fue la elección de servicios basados en la nube, optar por servicios como Microsoft y Onetrust, que funcionan en la nube, en lugar de instalar infraestructura tecnológica local. De esta forma se reduce la huella de carbono, ya que los centros de datos en la nube son más eficientes energéticamente que los servidores locales.

La segunda decisión fue un enfoque en pequeñas y medianas empresas (PYMES) para un mayor impacto social, diseñar la aplicación con un enfoque específico en PYMES que tienen menos recursos para invertir en soluciones avanzadas de seguridad de datos. Este planteamiento encuentra un nicho actual en el mercado y aborda una necesidad social al cerrar la brecha tecnológica entre empresas grandes y pequeñas.

Una vez explicadas las decisiones claves, se explica el impacto buscado a nivel personal, empresarial, social, económico, medioambiental y cultural.

A nivel personal

Hay numerosos colectivos de personas que se verían beneficiados de esta aplicación, especialmente responsables de recoger datos en empresas pequeñas experimentan menos estrés gracias a la automatización de procesos complejos y empleados tienen mayor confianza en el manejo de su información personal. Por tanto, estas personas consiguen reducir el estrés laboral, tener una mayor percepción de control y confianza y una formación indirecta al contar con nuevas medidas de protección de datos que son explicadas a los empleados.

Además, los clientes tienen un mayor sentimiento de seguridad cuando la empresa que solicita sus datos cuenta con certificaciones que confirman la seguridad de datos y su gestión adecuada. De esta forma, se consigue aportar una mayor percepción de control y confianza al saber que sus datos están protegidos según normativas avanzadas.

También para los responsables de cumplimiento legal (Data Protection Officers o similares) ya que la aplicación simplifica las tareas relacionadas con el cumplimiento normativo, lo que reduce su carga de trabajo y el estrés asociado a garantizar que la empresa cumpla con normativas complejas como el RGPD.

A nivel empresarial

Permite a las empresas confirmar el cumplimiento de normativas de protección de datos de manera más eficiente y a menor costo. Esto supone que garantiza el cumplimiento legislativo y posibles sanciones.

También permite una reducción de costos operativos al utilizar servicios en la nube, se eliminan gastos asociados a hardware, instalaciones y mantenimiento.

Además, aporta seguridad a las empresas ante posibles ciberataques que comprometan datos sensibles. Esto hace que la imagen de marca mejore gracias

a una mayor reputación empresarial por su responsable gestión de datos. Por tanto, aumenta la competitividad das empresas, atrayendo así a más clientes.

A nivel social

Esta aplicación contribuye a reducir las brechas tecnológicas y sociales entre empresas grandes y pequeñas, promoviendo un acceso más equitativo a herramientas tecnológicas. Reduce desigualdades tecnológicas ya que empresas pequeñas y medianas tienen acceso a herramientas que antes estaban reservadas para grandes corporaciones con mayores recursos.

Además, fomenta de la inclusión digital, empresas de sectores menos tecnificados pueden acceder a soluciones avanzadas, lo que aumenta su inclusión y fortalece comunidades locales al fomentar la equidad en el acceso a recursos.

A nivel económico

El uso de la aplicación minimiza costos operativos y legales, realiza auditorías para procesos comunes de varias empresas disminuyendo los costes. Además, al usar servicios en la nube que comparten recursos minimiza los gastos y consultas que debería hacer cada empresa por su cuenta.

Además, al cumplir la normativa las empresas usuarias reducen gastos legales y multas por incumplimiento, lo que permite reinvertir esos recursos en innovación o expansión, generando impacto positivo en la economía local. De esta forma, pueden reinvertir recursos gracias al ahorro en costos legales y tecnológicos que permite a las empresas reinvertir en áreas clave como innovación y marketing.

También aumenta la productividad por la automatización de procesos, que libera tiempo y recursos para que los empleados se centren en tareas de mayor valor añadido.

Finalmente, la incorporación de esta aplicación a una empresa fomenta el crecimiento empresarial ya que las empresas más seguras y eficientes pueden expandirse, generando empleos y aumentando su contribución al PIB.

A nivel medioambiental

El modelo basado en servicios en la nube reduce la necesidad de infraestructura física, disminuyendo el consumo energético y los residuos electrónicos. La aplicación evita que pequeñas empresas instalen servidores físicos, reduciendo emisiones de carbono asociadas al almacenamiento local y el transporte de hardware.

La huella de carbono es una medida del impacto ambiental que tienen las actividades humanas en términos de la cantidad de gases de efecto invernadero (GEI) emitidos, expresados generalmente en toneladas de dióxido de carbono equivalente (CO_2e). Incluye emisiones directas, como las generadas por vehículos o fábricas, y emisiones indirectas, como las asociadas a la producción de bienes, servicios y electricidad. Reducir la huella de carbono es crucial para combatir el cambio climático, ya que los GEI son responsables del calentamiento global. Las acciones para mitigar esta huella incluyen el uso de energías renovables, tecnologías más eficientes y modelos de negocio sostenibles.

Proyectos como el de esta aplicación que eliminan la necesidad de infraestructura física y utilizan servicios en la nube, reducen el número de

residuos electrónicos y fomentan la digitalización de procesos contribuyendo a reducir las emisiones que forman la huella de carbono.

A nivel cultural

El proyecto promueve una cultura empresarial más orientada a la seguridad digital y al cumplimiento normativo, fomentando prácticas éticas y responsables. Empresas adoptan estándares más altos en la gestión de datos, lo que refuerza una percepción cultural de la importancia de la privacidad y la seguridad en un mundo digitalizado. Promueve un cambio en la percepción de la seguridad digital ya que aumenta la conciencia de la importancia de proteger datos personales y de cumplir con normativas.

Además, fomenta la ética empresarial, refuerza valores como la transparencia y la responsabilidad en el manejo de información sensible. También crea hábitos digitales responsables, la facilidad de uso de la aplicación impulsa prácticas seguras en el entorno digital, tanto en las empresas como en los usuarios finales. Esto provoca una promoción de la educación tecnológica por la necesidad de adoptar estas soluciones fomenta el aprendizaje continuo sobre herramientas digitales y normativas.

7.1 Potencial del impacto basado en los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030

Los Objetivos de Desarrollo Sostenible (ODS) son un conjunto de 17 objetivos globales adoptados en 2015 por los Estados Miembros de las Naciones Unidas como parte de la Agenda 2030 para el Desarrollo Sostenible. Este marco establece un plan de acción global con metas específicas para erradicar la pobreza, proteger el planeta y garantizar la paz y prosperidad para todos, bajo la premisa de "no dejar a nadie atrás". Los ejes centrales de la Agenda 2030 son:

- Personas: Mejorar la calidad de vida y erradicar la pobreza.
- Planeta: Proteger el medio ambiente y combatir el cambio climático.
- Prosperidad: Promover el desarrollo económico sostenible y la igualdad.
- Paz: Fomentar sociedades justas, pacíficas e inclusivas.
- Alianzas: Impulsar la colaboración global para alcanzar los objetivos.

Figura 11: Objetivos de Desarrollo Sostenible

En concreto, los objetivos con los que se alinea la aplicación son con el doce, trece, diez, dieciséis, doce, ocho y nueve.

ODS 12: Producción y consumo responsables

El modelo basado en la nube optimiza el uso de recursos tecnológicos, minimizando el desperdicio y la necesidad de hardware adicional. Esto reduce los residuos electrónicos y el consumo energético. Las empresas que utilizan la aplicación pueden operar de manera más eficiente, reduciendo su impacto ambiental y fomentando prácticas responsables.

ODS 13: Acción por el clima

Al reducir la huella de carbono asociada a la gestión de infraestructura física y promover el uso de centros de datos eficientes, la aplicación contribuye a la mitigación del cambio climático. Refuerza la sostenibilidad de las empresas al integrar soluciones que reducen las emisiones de gases de efecto invernadero.

ODS 10: Reducción de las desigualdades

Al diseñarse para PYMES, la aplicación cierra brechas tecnológicas entre empresas grandes y pequeñas, garantizando que todas tengan acceso a soluciones modernas para proteger datos. Promueve la inclusión tecnológica al hacer que herramientas avanzadas sean accesibles para empresas con menos recursos.

ODS 16: Paz, justicia e instituciones sólidas

Proporciona herramientas que fortalecen la transparencia y el cumplimiento legal, especialmente en lo relacionado con la protección de datos. Esto fomenta prácticas empresariales éticas y responsables. Ayuda a generar confianza en los consumidores, promoviendo relaciones justas y sostenibles entre empresas y usuarios.

ODS 12: Producción y consumo responsables

El modelo basado en la nube optimiza el uso de recursos tecnológicos, minimizando el desperdicio y la necesidad de hardware adicional. Esto reduce los residuos electrónicos y el consumo energético. Las empresas que utilizan la aplicación pueden operar de manera más eficiente, reduciendo su impacto ambiental y fomentando prácticas responsables.

ODS 8: Trabajo decente y crecimiento económico

Proporciona a las empresas herramientas asequibles para cumplir con regulaciones, evitando sanciones y liberando recursos para reinvertir en el crecimiento empresarial. Facilita la creación de empleo especializado en gestión de datos, marketing digital y soporte técnico, promoviendo el empleo de calidad.

ODS 9: Industria, innovación e infraestructura

La aplicación fomenta la innovación tecnológica mediante el uso de servicios avanzados como Microsoft y OneTrust. Al promover soluciones basadas en la nube, apoya la construcción de infraestructuras digitales más sostenibles. Ayuda a pequeñas y medianas empresas (PYMES) a adoptar tecnología avanzada, aumentando su competitividad en sectores con altos niveles de innovación.

(NacionesUnidas, s.f.)

8 Bibliografía

CorporateFinanceInstitute. (s.f.). *Net Present Value (NPV).* Obtenido de https://corporatefinanceinstitute.com/resources/valuation/net-present-value-npv/

ESERP, D. B. (2022). Análisis PESTER de una empresa: qué es y cómo hacerlo. *ESERP Digital Business & Law School.* Obtenido de https://es.eserp.com/articulos/que-es-analisis-pestel/

ESIC. (2024). Ciclo de vida de los datos: qué es y cuáles son sus etapas. *ESIC Business.* Obtenido de https://www.esic.edu/rethink/tecnologia/ciclo-vida-datos-c

España, G. d. (s.f.). *España Digital 2025.* Obtenido de https://avancedigital.mineco.gob.es/programas-avance-digital/Paginas/espana-digital-2025.aspx

EuropeanInnovationCouncil. (29 de Octubre de 2024). *EIC 2025 work programme* . Obtenido de https://eic.ec.europa.eu/eic-2025-work-programme_en

Hargrave, M. (24 de julio de 2024). *Investopedia.* Obtenido de https://www.investopedia.com/terms/w/wacc.asp

IDC. (2021). *Security Spending Guide.* IDC.

INCIBE. (2022). *Análisis y dianóstico del talento de ciberseguridad en España.* INCIBE. Obtenido de https://files.incibe.es/incibe/talento/INCIBE_Resumen_DIAG.pdf

INCIBE. (s.f.). *Análisis y caracterización del mercado de Ciberseguridad.* INCIBE. Obtenido de https://www.incibe.es/sites/default/files/contenidos/blog/caracterizacion-mercado-ciberseguridad-spain/incibe-caracterizacion-mercado-ciberseguridad.pdf

IndustriaConectada4.0. (s.f.). *ACTIVA Ciberseguridad.* Obtenido de https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx

INESDI, B. t. (23 de 07 de 2021). *Marketing digital, ventajas y desventajas.* Obtenido de https://www.inesdi.com/blog/marketing-digital-ventajas-y-desventajas/

María de los Angeles Gil Estallo, F. G. (2007). *Cómo crear y hacer funcionar una empresa.* ESIC.

Ministerio de Industria y turismo, G. d. (septiembre de 2024). *Cifras PYME.* Obtenido de https://ipyme.org/Publicaciones/Cifras%20PYME/CifrasPyme-septiembre2024.pdf

Mónica, M. R. (22 de Octubre de 2021). *Statista.* Obtenido de https://es.statista.com/grafico/26031/volumen-estimado-de-datos-digitales-creados-o-replicados-en-todo-el-mundo/

NacionesUnidas. (s.f.). *Objetivos de Desarrollo Sostenible.* Obtenido de https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

onetrust. (s.f.). *Productos onetrust*. Obtenido de https://www.onetrust.com/es/products/

Secretaría de Estado de Seguridad, G. d. (2022). *Informe sobre la cibercriminalidad en España.* Obtenido de https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2022_126200212.pdf

SegurdidadSocial. (2024). *Bases y tipos de cotización 2024*. Obtenido de https://www.seg-social.es/wps/portal/wss/internet/Trabajadores/CotizacionRecaudacionTrabajadores/36537

Triquels. (10 de Febrero de 2020). *Canvas social: qué es y cómo te puede ayudar con tu proyecto sostenible + PLANTILLA*. Obtenido de https://www.triquels.com/blog/canvas-social

Unión Europea. (2016). *Reglamento General de Protección de Datos (Reglamento UE 2016/679).* Diario Oficial de la Unión Europea, L 119, pp. 1-88.

Valencia, C. (2021). *Sostenibilidad para los negocios*. Obtenido de https://negociosostenible.camaravalencia.com/ambiental/tendencias/que-es-la-huella-de-carbono-digital/

Vipong, T. (s.f.). *corporatefinanceinstitute.* Obtenido de https://corporatefinanceinstitute.com/resources/valuation/internal-rate-return-irr/

9 Anexos

9.1 Anexo I: Factura de pruebas Microsoft Purview

Para la estimación de costes de las herramientas de Azure se utiliza la herramienta Azure Pricing Calculator. Tras introducir los datos, estima los costes y se incluyen en la siguiente figura:

Microsoft Azure Estimate					
Su presupuesto					
Service category	**Service type**	**Region**	**Description**	**Estimated monthly cost**	**Estimated upfront cost**
Administración y Gobernanza	Microsoft Cost Management		Sin cargo por el gasto administrado de Azure. 0 Gasto administrado de AWS al mes	$0,00	$0,00
Análisis	Microsoft Purview	Spain Central	Mapa de datos de Microsoft Purview, Examen y clasificación automatizados: 1 de duración total del examen en minuto x 32 núcleos virtuales en total entre todos los exámenes (para otros orígenes de datos), Data Map Enrichment: 730 Advanced Resources Set horas, 730 Report Generation Horas, Mapa de datos elástico: 1 unidades de capacidad hora, 730 horas, Microsoft Purview Applications, Data Catalog: C0 Service, Data Policy: 50 DevOps Policies x 730 Horas, Insight Consumption: 200 API calls	$1.192,82	$0,00
Support		**Support**		$29,00	$0,00
		Licensing Program	**Microsoft Customer Agreement (MCA)**		
		Billing Account			
		Billing Profile			
		Total		**$1.221,82**	**$0,00**

Enlace al Excel completo:

ExportedEstimate(1).xlsx

9.2 Anexo II: Resultados de consulta al banco Santander

Para tener un referente de los tipos de interés se usa este simulador

9.3 Anexo III: Excel con cuentas financieras

Este anexo cuenta con los cálculos utilizados en el apartado de financiación.

Flujos de caja Operativa					
Concepto	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**
Saldo año anterior		-108,570	-76,000	42,430	160,860
Entradas de efectivo					
Fondos propios	90				
Ventas del servicio	0	231,84	317,95	317,95	317,950
Total Entradas	90	231,84	317,95	317,95	317,950
Salidas de efectivo				0	0,000
Sueldos (contado SS)	-138,6	-138,6	-138,6	-138,6	-138,600
Herramientas (Microsoft/Onetrust)	-21,97	-23,97	-25,97	-25,97	-25,970
Campañas de marketing	-16,6	-14,6	-12,6	-12,6	-12,600
Asesoría legal	-3,4	-4	-4,25	-4,25	-4,250
Reserva para imprevistos	-18	-18,1	-18,1	-18,1	-18,100
Total Salidas	-198,570	-199,27	-199,52	-199,52	-199,520
Flujo Neto	-108,570	-76,000	42,430	160,860	279,290

Flujos de caja Financiera			
Concepto	**Año 0**	**Año 1**	**Año 2**
Salidas año anterior		116,412	80,427
Entradas			
Préstamos	119,341	118,357	
Total Entradas	119,341	234,769	80,427
Salidas			
Intereses del préstamo	-2,929	-8,494	-2,305
Pagos del préstamo		-145,848	-91,849
Total Salidas	-2,929	-154,342	-94,154
Flujo Neto	116,412	80,427	-13,727

Flujos de caja Totales				
Concepto	**Año 0**	**Año 1**	**Año 2**	**Año n**
Flujo Operativo	-108,57	-76	42,43	160,86
Flujo Financiero	116,412	80,427	-13,727	
Total	7,842	4,427	28,703	160,86

Cuenta de pérdidas y ganancias			
Concepto	**Año 0**	**Año 1**	**Año 2**
Ingresos			
Ventas del servicio	0	231,84	317,95
Total Ingresos	0	231,84	317,95
Costos Directos			
Sueldos	-138,6	-138,6	-138,6
Herramientas (Microsoft/Onetrust)	-21,97	-23,97	-25,97
Campañas de marketing	-16,6	-16,6	-16,6
Formularios y Asesoría legal	-3,4	-4	-4,25
Total Costos Directos	-180,57	-183,17	-185,42
Costos Financieros			
Intereses del préstamo	0,000	-8,494	-2,305
Total Costos Financieros	0	-8,494	-2,305
Resultado Operativo	-180,57	40,176	130,225
Reserva para imprevistos	-18	-18,1	-18,1
Resultado Neto	-198,57	22,076	112,125

Año 1				
Servicio	Clientes	Tarifa Mensual (€)	Ingresos Mensuales (€)	Ingresos Anuales (€)
Servicio mínimo	20	300	6	72
Servicio básico	15	500	7,5	90
Servicio experto	10	800	8	96
Servicio completo	5	1,22	6,1	73,2
Total	50	-	27,6	331,2

Año 2				
Servicio	Clientes	Tarifa Mensual (€)	Ingresos Mensuales (€)	Ingresos Anuales (€)
Servicio mínimo	24	300	7,2	86,4
Servicio básico	18	500	9	108
Servicio experto	12	800	9,6	115,2
Servicio completo	6	1,22	7,32	87,84
Total	60	-	33,12	397,44

Valores	
E (Capital propio):	90000
D (Deuda):	119341,2
Re (Costo del capital propio):	15%
Rd (Costo de la deuda):	5,45%
T (Tasa impositiva):	25%
V (Valor total): E+D.	209341,2
WACC	8,78%
VAN	167,1850
TIR	37%

cuentas_financiación.xlsx

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=ETS Ingenieros Informaticos - UPM, C=ES
	Fecha/Hora	Tue Jan 14 17:16:16 CET 2025
	Emisor del Certificado	EMAILADDRESS=camanager@etsiinf.upm.es, CN=CA ETS Ingenieros Informaticos, O=ETS Ingenieros Informaticos - UPM, C=ES
	Numero de Serie	561
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)