

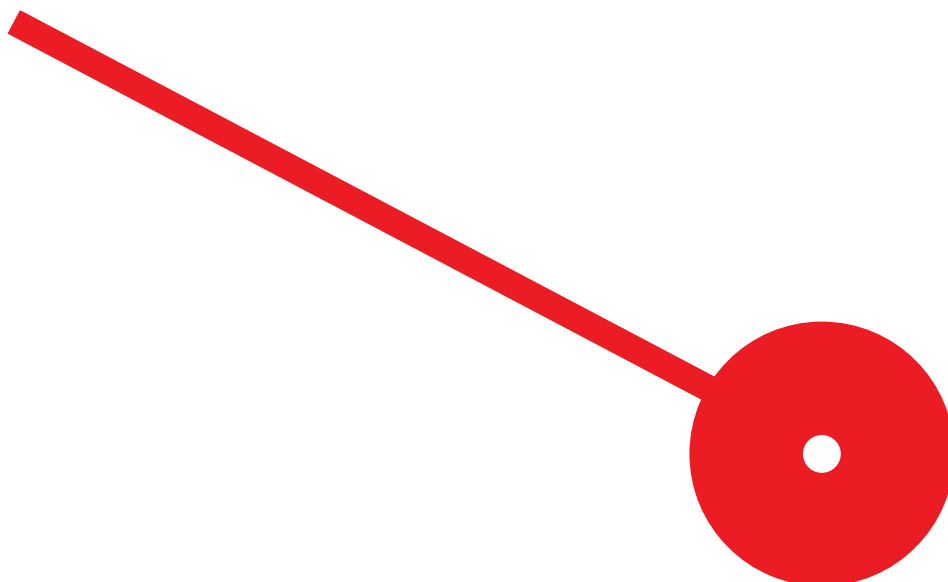


Conceção de um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe.

Omar David Bouabe Soares

VERSÃO FINAL

06/2025





Conceção de um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe.

Omar David Bouabe Soares

**Dissertação de Mestrado apresentado ao Instituto Superior de
Contabilidade e Administração do Porto para a obtenção do grau de
Mestre em Negócio Eletrónico, sob orientação de Professor Doutor
José Agostinho de Sousa Pinto**

Omar David Bouabe Soares. Conceção de um
Modelo de Negócio no Setor da Segurança Digital:

O caso KIS – Keep It Safe.

06/2025

Dedicatória

Dedico esta dissertação, e tudo o que ela representa, àqueles que me acompanharam, inspiraram e sustentaram ao longo de um caminho que, apesar de desafiante, foi profundamente transformador.

À minha família, que esteve sempre presente, mesmo quando a distância era feita de “horários apertados”, dias exaustivos e semanas em que quase não sobrava tempo para nada. Por todo o suporte constante, pelos conselhos sábios que tantas vezes me guiaram nos momentos de dúvida, e por todos os esforços silenciosos que fizeram, muitas vezes abdicando de conforto, de tempo e de tranquilidade, para que eu pudesse seguir este caminho. Agradeço-vos por terem compreendido as ausências, apoiado as minhas escolhas e por nunca me terem deixado esquecer quem eu sou, mesmo nos momentos em que me sentia apenas estudante e trabalhador, em “piloto automático”.

O vosso apoio, paciência e força deram-me os alicerces para continuar quando o cansaço ameaçava vencer. Este esforço é também, por vós. E é, também, um gesto de partilha com o meu irmão, André Karim Bouabe Soares, alguém tão empenhado e resiliente quanto eu, que mesmo quando os objetivos parecem distantes ou inatingíveis, com sacrifício e persistência, as coisas acontecem. Que este percurso sirva como prova e também como promessa, os objetivos tornam-se reais quando caminhamos com determinação e propósito.

Ao meu orientador, Professor Doutor José Agostinho de Sousa Pinto, não apenas pela orientação prestada, mas por ter confiado em mim desde o início. Por ter acreditado no meu potencial e se ter disponibilizado para me acompanhar, mesmo quando não existia tempo para o fazer. A sua excecional disponibilidade, confiança demonstrada e orientação foram elementos fundamentais para que este trabalho e fim de percurso pudessem ser concretizados com qualidade e significado.

À minha noiva, Maria Luís Machado Martins, que não foi apenas uma companheira de jornada, mas foi a origem dela. Foi ela quem me incentivou, com convicção e carinho, a retomar os estudos, quando a ideia de regressar aos 25 anos parecia improvável, longínqua e incerta. A cada passo, partilhou comigo os sacrifícios, as escolhas difíceis e o impacto que tudo isto teve na nossa vida pessoal.

Viveu comigo os desafios, abdicou de tanto quanto eu, e nunca deixou de estar ao meu lado, mesmo quando o tempo que tínhamos era escasso e a exaustão era constante. Esta conquista é, também dela, pela força silenciosa que me deu todos os dias, pela paciência incondicional e por acreditar em mim quando eu ainda o estava a aprender.

Dedico também esta dissertação a mim. Ao jovem que decidiu contrariar o tempo, que recomeçou a vida académica mais tarde, já com responsabilidades acumuladas, e que escolheu não desistir mesmo quando tudo parecia exigir que o fizesse. Que trabalhou e estudou em simultâneo durante anos, que cedeu tempo, conforto e tranquilidade em nome de um objetivo maior. Que aprendeu que a persistência constrói mais do que o talento, e que os caminhos difíceis tornam, no fim, a meta ainda mais valiosa. Esta é, também, a vitória de quem soube resistir.

Concluir este Mestrado não é apenas alcançar uma meta académica. É o encerramento de um ciclo construído com esforço, sacrifício e determinação e o início de um novo capítulo com mais maturidade, mais ferramentas e, sobretudo, com a consciência de que vale sempre a pena lutar por aquilo em que acreditamos.

Agradecimentos

Ao concluir esta etapa marcante da minha vida académica e pessoal, não posso deixar de expressar a minha profunda gratidão a todos os que, direta ou indiretamente, contribuíram para a concretização desta dissertação.

Agradeço, em primeiro lugar, ao meu orientador, Professor Doutor José Agostinho de Sousa Pinto, pela excepcional disponibilidade, orientação crítica e confiança desde o início deste percurso. A sua decisão de aceitar orientar este trabalho, representou para mim não só uma oportunidade, mas também um sinal de reconhecimento e incentivo que muito valorizei. O seu acompanhamento foi determinante para o sucesso deste projeto.

À minha família, pela paciência e apoio incondicional ao longo de todos estes anos. Pelos conselhos sábios, pelas cedências silenciosas e pelos sacrifícios feitos em meu nome, que muitas vezes passaram despercebidos, mas nunca foram tomados como garantidos. Em especial, ao meu irmão, cuja determinação tanto admiro, e a quem espero que este caminho possa também servir de inspiração.

À minha noiva, que esteve presente desde o primeiro dia desta jornada académica. Foi ela quem me incentivou a retomar os estudos e quem caminhou comigo lado a lado, mesmo nas fases mais difíceis. Pela compreensão constante, pela força transmitida nos momentos de cansaço e por nunca ter deixado de acreditar em mim, a minha gratidão será sempre insuficiente face ao que me deste.

Aos participantes do Focus Group, Professores Doutores José Agostinho de Sousa Pinto, Pedro Mendonça, Rui Umberto e Luís Rodrigues, pela generosidade com que aceitaram o convite, pela qualidade dos seus contributos e pela forma empenhada e construtiva como participaram na análise e validação do modelo de negócio proposto. As suas reflexões permitiram elevar significativamente a qualidade deste trabalho, tanto ao nível conceptual como estratégico.

Por fim, ao Instituto Superior de Contabilidade e Administração do Porto (ISCAP), pela qualidade do ensino e pelo ambiente que fomentou o rigor, a inovação e a ligação entre o conhecimento académico e a sua aplicação no mundo real.

A todos o meu mais sincero obrigado.

Resumo:

A presente dissertação propõe o desenvolvimento e avaliação da viabilidade do KIS – *Keep It Safe*, um dispositivo de segurança digital concebido para responder aos desafios crescentes da cibersegurança, com foco na autenticação biométrica, gestão de acessos e proteção de criptoativos e o seu respetivo modelo de negócios. A motivação decorre da necessidade de soluções fiáveis, intuitivas e eficazes, perante o aumento dos ataques digitais e a fragilidade dos métodos tradicionais de autenticação.

O KIS combina num único hardware tecnologias de segurança, nomeadamente criptografia de nível militar, sensor de impressão digital de alta precisão e conectividade. Incorpora um firmware otimizado, integração com protocolos de autenticação multifatorial e funcionalidades de backup local e em nuvem, que asseguram compatibilidade com os principais sistemas operativos e infraestruturas empresariais.

A vertente prática do trabalho estrutura-se através da construção de um modelo e plano de negócios, que engloba a análise de mercado, proposta de valor, segmentação de clientes B2B (“Business to Business” ou “Empresa para Empresa”) e B2C (“Business to Consumer” ou “Empresa para Consumidor”), análise da concorrência, estratégia comercial, canais de distribuição, estrutura de custos e projeções financeiras a cinco anos.

Conclui-se que o KIS e o seu respetivo plano de negócios oferecem uma solução inovadora, escalável e sustentável, com elevado potencial de adoção nos mercados nacional e internacional. A sua proposta única, que alia segurança, utilização e integração tecnológica, poderá posicioná-lo como uma referência no domínio da segurança digital pessoal e corporativa.

Palavras chave: Segurança, Gestão de acessos, Criptoativos, Inovação Tecnológica

Abstract:

This dissertation proposes the development and feasibility assessment of KIS – *Keep It Safe*, a digital security device designed to address the growing challenges of cybersecurity, with a focus on biometric authentication, access management, and cryptoasset protection and its respective business model. The motivation stems from the need for reliable, intuitive, and effective solutions in response to increasing digital threats and the inherent weaknesses of traditional authentication methods.

KIS combines several security technologies into a single hardware device, including military-grade encryption, a high-precision fingerprint sensor, and versatile connectivity. It incorporates optimized firmware, integration with multifactor authentication protocols, and both local and cloud-based backup functionalities, ensuring compatibility with major operating systems and enterprise infrastructures.

The practical component of the work is developed through the construction of a comprehensive business model and plan, which include market analysis, value proposition, B2B and B2C customer segmentation, competitive benchmarking, commercial strategy, distribution channels, cost structure, and five-year financial projections.

It is concluded that KIS and his business plan offers an innovative, scalable, and sustainable solution, with high potential for adoption in both national and international markets. Its unique value proposition — combining security, usability, and technological integration — may position it as a benchmark in the field of personal and corporate digital security.

Key words: Security, Access management, Cryptoassets, Technological innovation

Índice geral

Capítulo - Introdução	1
Capítulo I – Enquadramento da Investigação	4
1 Contextualização	5
1.1 Enquadramento e Motivação	5
1.2 Problemática	7
1.3 Objetivos e Resultados Esperados	9
1.4 Abordagem Metodológica	11
1.5 Estrutura do Documento.....	14
Capítulo II – Estado da Arte	16
2 Revisão de literatura	18
2.1 Business Model Canvas.....	18
2.2 Metodologia <i>Focus Group</i>	22
2.3 Memorização de Palavras-passe	24
2.4 Proteção por Biometria.....	25
2.5 Proteger criptoativos em “ <i>cold wallets</i> ”	27
2.6 Segurança e Privacidade de Dados	29
2.7 Palavras-passe seguras.....	30
Capítulo III –Abordagem metodológica	32
3 Abordagem metodológica.....	33
3.1 Questão/Problema da Investigação.....	33
3.2 Objetivo da Investigação	34
3.3 Metodologia da Investigação.....	35
Capítulo IV –Focus Group	37
4 Focus Group – Modelo de Negócio KIS	38
4.1 Estrutura do Plano de Negócios antes do Focus Group.....	39
4.2 Estrutura e Realização do Focus Group	42

4.3	Resultados.....	44
4.4	Ajustes e Decisões Estratégicas.....	54
Capítulo V – Conclusões e Perspetivas de Desenvolvimento.....		58
5	Contributos da Investigação	60
5.1	Síntese dos Resultados.....	63
5.2	Dificuldades e Limitações do Trabalho.....	64
5.3	Trabalhos Futuros	66
Referências bibliográficas.....		68
Apêndice		71
	Apêndice I – Plano de Negócios.....	72
Anexo		145
	Anexo I – Guião do Focus Group	146

Índice de Figuras

Figura 1 - Dispositivo KIS	5
Figura 2 - Embalagem do dispositivo KIS	55
Figura 3 - Logo KIS	98
Figura 4 - Logótipo e Marca.....	141
Figura 5 - KIS - Visão Frontal e ecrã ligado	142
Figura 6 - KIS - Visão Traseira	142
Figura 7 - KIS – Visão Diagonal Frontal	143
Figura 8 - KIS - Visão diagonal traseira esquerda	143
Figura 9 – KIS - Visão diagonal traseira direita.....	144
Figura 10 – Embalagem e selo	144

Índice de Tabelas

Tabela 1 - Comparação da Concorrência.....	81
Tabela 2 - Mapa de Custo de Mercadorias Vendidas e Matérias Consumidas	120
Tabela 3 - Fornecimento e Serviços Externos	121
Tabela 4 - Custos com o Pessoal	122
Tabela 5 - Investimentos.....	122
Tabela 6 - Arrendamento do Espaço	123
Tabela 7 - Simulação do Financiamento a 5 anos	124
Tabela 8 - Demonstração de Resultados (5 Anos).....	125
Tabela 9 - Cash-Flow de Exploração (5 Anos)	128
Tabela 10 - Necessidades de Fundo de Maneio (NFM)	129
Tabela 11 - Valor Residual (5º Ano)	130
Tabela 12 - Cash-Flow de Investimento (5 Anos).....	132
Tabela 13 - Cash-Flow Global (5 Anos).....	133
Tabela 14 - Mapa de Vendas (5 Anos)	135
Tabela 15 - Plano Financeiro (5 Anos).....	137
Tabela 16 - Rentabilidade (5 anos).....	138
Tabela 17 - Balanço (5 Anos).....	139

Lista de abreviaturas

KIS - Keep It Safe (Nome do dispositivo – “Mantem em Segurança”)

B2B - Business to Business (Empresa para Empresa)

B2C - Business to Consumer (Empresa para Consumidor)

MFA - Multi-Factor Authentication (Autenticação Multifatorial)

NFM - Necessidades de Fundo de Maneio

PI - Patente de Invenção

CMVMC - Custo de Mercadorias Vendidas e Matérias Consumidas

KPIs - Key Performance Indicators (Indicadores-Chave de Desempenho)

ERP - Enterprise Resource Planning (Planeamento de Recursos Empresariais)

SLA - Service Level Agreement (Acordo de Nível de Serviço)

ROI - Return on Investment (Retorno do Investimento)

CAC - Custo de Aquisição de Cliente

USB-C - Universal Serial Bus – Type C

NFC - Near Field Communication (Comunicação por Campo de Proximidade)

LiPo - Lithium Polymer (Tipo de bateria de polímero de lítio)

TI - Tecnologias da Informação

CAPÍTULO - INTRODUÇÃO

A crescente digitalização dos processos organizacionais e da vida quotidiana tem reforçado a importância da segurança da informação como um fator crítico de sucesso. À medida que se intensificam as ameaças digitais, tanto os utilizadores individuais como as organizações enfrentam desafios significativos na proteção de dados sensíveis, na gestão de acessos e na salvaguarda dos seus ativos digitais, nomeadamente criptoativos. Neste contexto, torna-se cada vez mais necessário o desenvolvimento de soluções de segurança integradas, que aliem eficácia técnica, simplicidade na sua utilização e viabilidade comercial.

Através desta problemática, esta dissertação centra-se na análise do modelo de negócio associado ao KIS – Keep It Safe, um dispositivo multifuncional concebido para garantir a gestão segura de acessos e ativos digitais, através de autenticação biométrica.

Ao invés de se focar no desenvolvimento técnico do produto, a investigação privilegia a definição da estrutura estratégica do modelo de negócios subjacente, com o objetivo de compreender em que medida esta proposta de valor poderá ser viável e competitiva num mercado em expansão, tanto no segmento de consumidores individuais (B2C) como no segmento empresarial (B2B) através da técnica de pesquisa qualitativa “*Focus Group*”.

Neste enquadramento, a questão de investigação que orienta a presente dissertação é: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep it Safe?” Esta questão remete para uma abordagem centrada na análise dos nove elementos que compõem o Business Model Canvas, enquanto ferramenta conceptual de apoio à construção e representação de modelos de negócio inovadores.

A abordagem metodológica adotada para a respetiva validação é de natureza qualitativa e tem como principal técnica de validação e recolha de dados a realização de um Focus Group. Esta técnica foi aplicada junto de um painel composto por quatro Professores Doutores do Instituto Superior de Contabilidade e Administração do Porto (ISCAP), com experiência académica e profissional nas áreas da gestão, sistemas de informação, inovação tecnológica e desenvolvimento de modelos de negócio.

A escolha deste método justifica-se pela sua adequação à exploração de perceções, interpretações e juízos críticos sobre a viabilidade da proposta apresentada.

O modelo de negócio foi analisado nos seus diversos elementos, com exceção do componente relativo à estrutura de custos, dado que este projeto se insere no âmbito de uma dissertação de Mestrado e por esse motivo os valores presentes no plano de negócios são meramente especulativos.

O objetivo geral da dissertação consiste, assim, em analisar e validar um modelo de negócio sustentável para a solução KIS, ao ter como base a aplicação sistemática do Business Model Canvas, com especial atenção às especificidades dos segmentos B2B e B2C.

A investigação possui como objetivos específicos, caracterizar as funcionalidades mais valorizadas pelos potenciais utilizadores do KIS, compreender o impacto da autenticação exclusivamente biométrica na perceção de segurança e privacidade dos utilizadores, analisar a atratividade da proposta de valor do produto nos contextos pessoal (B2C) e empresarial (B2B), aferir o grau de aceitação de um modelo de subscrição associado a serviços adicionais e funcionalidades premium e identificar as principais barreiras à adoção do produto, ao propor recomendações para a sua mitigação e superação, o que deste modo, contribui para a compreensão do potencial comercial da solução.

A estrutura da dissertação compreende, para além da presente introdução, a revisão da literatura relevante, a caracterização detalhada da solução tecnológica, a aplicação prática do Business Model Canvas, a análise dos contributos obtidos através do Focus Group, a discussão crítica dos resultados e o plano de negócios (apêndice I).

Ao posicionar-se na interseção entre a segurança digital e a inovação de modelos de negócio, esta dissertação pretende contribuir para o avanço do conhecimento no domínio do negócio eletrónico, ao demonstrar como uma solução emergente pode ser estruturada de forma sólida, validada por especialistas e projetada para competir num mercado exigente e em constante transformação.

CAPÍTULO I – ENQUADRAMENTO DA INVESTIGAÇÃO

1 Contextualização

1.1 Enquadramento e Motivação

A transformação digital tem promovido uma mudança estrutural nas interações humanas, nas práticas organizacionais e na forma como a informação é gerada, armazenada e partilhada. A crescente interdependência entre pessoas, sistemas e infraestruturas digitais tem intensificado a exposição a riscos virtuais, na qual os ataques informáticos, o roubo de dados e a usurpação de identidade tem se tornado fenómenos cada vez mais frequentes e sofisticados. Neste contexto, a cibersegurança assume-se como um domínio estratégico e transversal, cuja relevância ultrapassa a esfera técnica, ao impactar diretamente a confiança dos utilizadores, a integridade dos ativos digitais e a sustentabilidade das organizações.

Um dos principais desafios contemporâneos no domínio da segurança digital reside na gestão de identidades e acessos. A utilização de palavras-passe frágeis, a sua reutilização em múltiplas plataformas e a ausência de mecanismos de verificação fortes constituem pontos de falha comuns, explorados por agentes maliciosos com facilidade crescente. Paralelamente, a ascensão dos criptoativos como forma de investimento e instrumento de transação exige novas abordagens para a sua custódia, dado o carácter descentralizado e irreversível das transações em redes blockchain. Estes fatores convergem para a necessidade de soluções integradas, que conciliem segurança, praticidade e adaptabilidade às diversas realidades digitais.

É neste enquadramento que surge o projeto KIS – *Keep It Safe*, cujo principal objetivo consiste no desenvolvimento e validação de um modelo de negócio inovador sustentado num dispositivo físico multifuncional. O KIS visa incorporar, num único produto, funcionalidades de autenticação biométrica, gestão de acessos e armazenamento seguro de criptoativos:



Figura 1 - Dispositivo KIS

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D AutoCAD

Todavia, esta dissertação não se limita à análise técnica do dispositivo, o foco central recai na estruturação e avaliação do modelo de negócio que viabilize a sua disponibilização e comercialização em larga escala, com base em pressupostos estratégicos, económicos e operacionais. A motivação para a realização deste estudo assenta em diversos fatores complementares.

Em primeiro lugar, verifica-se uma lacuna no mercado relativamente a soluções que conjuguem múltiplos níveis de proteção com uma experiência de utilização simples e intuitiva. As soluções atualmente disponíveis tendem a especializar-se em componentes isoladas da segurança digital, algumas focam-se exclusivamente na gestão de palavras-passe, outras oferecem proteção avançada para criptoativos, mas sem considerar a autenticação de acessos, outras ainda são exclusivamente baseadas em software, dependentes da cloud e vulneráveis a falhas de rede ou violações de dados. Assim, embora eficazes nos seus domínios, estas soluções não oferecem uma abordagem integrada e física que garanta simultaneamente a segurança de acessos, a proteção de ativos digitais e a autenticação forte. A ausência de multifuncionalidade, a fragmentação da experiência do utilizador e a dependência de terceiros são limitações frequentemente identificadas nas opções concorrentes.

Em segundo lugar, a análise do mercado revela uma procura crescente por soluções de segurança portáteis, interoperáveis e que respeitem os princípios da proteção de dados, conforme estabelecido, por exemplo, no Regulamento Geral sobre a Proteção de Dados (RGPD) em vigor na União Europeia. A preferência por soluções que assegurem a autonomia do utilizador, evitem o armazenamento na nuvem e proporcionem uma experiência offline segura reflete uma tendência crescente entre consumidores conscientes dos riscos de segurança digital.

Adicionalmente, o crescente interesse dos consumidores individuais e empresas na adoção de práticas mais seguras de acesso e gestão de informação sensível cria uma oportunidade para os modelos de negócio com segmentação simultânea B2C e B2B, capazes de responder às especificidades de diferentes segmentos de mercado.

No caso do B2C, destaca-se a procura por soluções que simplifiquem a vida digital do utilizador comum, de forma a reduzir a complexidade associada à gestão de credenciais e a aumentar a proteção de dados pessoais.

No segmento B2B, observa-se uma necessidade urgente de ferramentas que permitam às organizações controlar o acesso a sistemas internos de forma automatizada, escalável e auditável, sobretudo em contextos de elevada rotatividade de recursos humanos ou ambientes regulados.

Neste panorama, a proposta do KIS distingue-se pela sua arquitetura integrada e pelo facto de responder simultaneamente às três grandes exigências do setor: segurança física robusta, usabilidade elevada e autonomia operacional. O dispositivo propõe-se colmatar as lacunas identificadas nos produtos concorrentes, apresentando-se como uma solução híbrida, portátil, independente de servidores externos e centrada no utilizador, com aplicação tanto em contextos pessoais como organizacionais. A presente dissertação pretende, assim, contribuir para o avanço do conhecimento na interseção entre o negócio eletrónico, a inovação tecnológica e a cibersegurança, ao apresentar um modelo de negócio baseado em tecnologia de segurança, com forte componente de diferenciação e potencial de internacionalização.

1.2 Problemática

A crescente digitalização das atividades humanas e económicas tem trazido benefícios significativos em termos de conectividade, produtividade e acesso à informação. No entanto, esta evolução tem sido acompanhada por uma intensificação das ameaças no domínio da cibersegurança, que colocam em risco os dados pessoais, ativos financeiros digitais e infraestruturas críticas. A gestão de acessos, o controlo de acessos e a proteção de criptoativos tornaram-se desafios centrais tanto para os utilizadores individuais como para as organizações.

Em paralelo, a proliferação de soluções tecnológicas no mercado tem dado origem a um ecossistema fragmentado, no qual coexistem aplicações especializadas em autenticação multifatorial, carteiras de criptoativos, plataformas de gestão de identidade e ferramentas de encriptação de dados.

Estas soluções, embora tecnicamente eficazes nos seus domínios específicos, revelam-se frequentemente complexas, pouco interoperáveis e difíceis de integrar numa experiência de utilização coesa e segura.

Tal situação representa um entrave significativo à adoção generalizada de boas práticas de segurança digital, sobretudo por parte de utilizadores não especializados ou de pequenas e médias empresas. Para além dos desafios técnicos, uma das principais dificuldades impostas é a dificuldade de estruturar um plano de negócios consistente que permita transformar estas soluções em propostas viáveis do ponto de vista comercial. A criação de um modelo de negócio eficaz, que contemple desde a proposta de valor até à estratégia comercial, representa um obstáculo que, quando negligenciado, compromete a concretização e sustentabilidade de projetos tecnologicamente promissores.

Neste enquadramento, a presente dissertação procura explorar, com recurso à metodologia “*Focus Group*”, o contributo desta abordagem para a identificação de elementos críticos que sustentem a definição e validação do modelo de negócio associado à proposta de conceção de um dispositivo multifuncional que, de forma integrada, combina a autenticação biométrica, gestão segura de acessos e o armazenamento de criptoativos.

No entanto, a problemática não se esgota na engenharia e implementação da solução tecnológica.

Para que esta possa ser viável no mercado, é imperativo definir e validar um modelo de negócio eficaz, que sustente a sua produção, comercialização e crescimento a longo prazo. A ausência de um modelo de negócios claramente definido é um dos principais fatores que inviabiliza a transição de soluções tecnológicas inovadoras para o mercado. A viabilidade de uma solução como o KIS depende não só da sua segurança e funcionalidade técnica, mas também da sua capacidade de gerar valor para os diferentes segmentos de utilizadores, de se posicionar estrategicamente face à concorrência e de garantir sustentabilidade económica e escalabilidade comercial.

Assim, o desafio que esta dissertação pretende explorar pode ser formulado da seguinte forma: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep it Safe?”

Esta questão implica uma abordagem multidimensional, que articule conhecimentos das áreas da cibersegurança, da inovação tecnológica, do marketing estratégico e da gestão empresarial.

A resposta exige não apenas uma fundamentação teórica e técnica sólida, mas também uma estruturação da proposta de valor, da segmentação de clientes, das estratégias de distribuição e dos indicadores financeiros que irão suportar a tomada de decisão empresarial.

Desta forma, a presente dissertação pretende contribuir para a resolução de um problema real e atual, ao propor uma solução integrada de segurança digital, com forte potencial de diferenciação no mercado, sustentada por um modelo de negócio tecnicamente fundamentado e comercialmente viável.

1.3 Objetivos e Resultados Esperados

A presente dissertação tem como propósito central a investigação do processo de conceção e implementação de um dispositivo multifuncional de segurança digital, designado por KIS, que visa integrar autenticação biométrica, gestão segura de acessos e armazenamento de criptoativos. Esta proposta nasce da necessidade de responder, de forma integrada, aos desafios emergentes no domínio da cibersegurança, nomeadamente no que respeita à proteção de credenciais, controlo de acessos e salvaguarda de ativos digitais descentralizados, como é o caso das criptomoedas.

Contudo, a originalidade e o contributo científico deste trabalho não se esgotam na dimensão técnica do produto, mas estendem-se, de forma destacada, à conceção e validação de um modelo de negócios viável, sustentável e escalável, capaz de suportar a introdução e a difusão da solução no mercado atual.

O objetivo geral deste estudo consiste, assim, em responder à seguinte questão de investigação: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?”, ao estruturar um modelo de negócio viável, sustentável e alinhado com as necessidades do mercado da segurança digital.

A presente dissertação propõe uma abordagem interdisciplinar que, embora parta de uma solução tecnológica, privilegia a dimensão estratégica e comercial da sua viabilização, ao articular conhecimentos provenientes das áreas da inovação tecnológica, do marketing, da gestão empresarial e do negócio eletrónico.

Procura-se, deste modo, demonstrar que é possível transformar uma proposta tecnológica complexa numa solução comercialmente viável, que gere valor para os seus utilizadores e que se diferencie no ecossistema competitivo da segurança digital.

Para alcançar este objetivo central, a investigação contempla diversos objetivos específicos, nomeadamente: caracterizar as funcionalidades mais valorizadas pelos potenciais utilizadores do KIS, compreender o impacto da autenticação exclusivamente biométrica na perceção de segurança e privacidade dos utilizadores, analisar a atratividade da proposta de valor do produto nos contextos pessoal (B2C) e empresarial (B2B), aferir o grau de aceitação de um modelo de subscrição associado a serviços adicionais e funcionalidades premium e identificar as principais barreiras à adoção do produto, ao propor recomendações para a sua mitigação e superação.

Neste enquadramento, torna-se fundamental compreender as expectativas, necessidades e reservas de potenciais utilizadores em relação ao KIS. Para tal, será adotada uma metodologia de investigação qualitativa, centrada na aplicação da técnica de *Focus Group*, cuja origem remonta às contribuições de Robert K. Merton e Paul Lazarsfeld, e que tem sido amplamente utilizada em contextos de desenvolvimento de produtos e na análise e validação de perceções subjetivas.

Esta técnica permite aceder a um conhecimento aprofundado das opiniões e motivações dos participantes, através de um ambiente de interação controlada, em que se estimula a partilha, a reflexão crítica e a construção coletiva de sentido em torno de uma temática específica.

As questões formuladas para o *Focus Group* visam obter informação diretamente aplicável à definição da proposta de valor e à formulação do modelo de negócio.

Entre os tópicos a explorar, incluem-se a identificação das funcionalidades mais relevantes do dispositivo KIS, sugestões de melhorias ou funcionalidades adicionais consideradas pertinentes, perceções sobre a confiança ou eventuais reservas quanto à autenticação biométrica como alternativa às palavras-passe, avaliação da proposta de valor enquanto fator motivador de aquisição, disponibilidade para aderir a um modelo de subscrição por serviços complementares, identificação de barreiras à adoção e recomendações para superá-las, quer do ponto de vista do produto, quer da estratégia de mercado.

Os resultados esperados com esta investigação incluem, em primeiro lugar, a obtenção de dados empíricos relevantes para a validação da proposta de valor e do modelo de negócio do KIS. Espera-se também identificar oportunidades concretas de melhoria da solução tecnológica, com base nas necessidades reais do mercado, bem como validar as premissas estratégicas que sustentam o plano de negócios.

Neste sentido, a análise qualitativa será complementada por uma modelação económico-financeira do projeto, com recurso a indicadores clássicos de viabilidade económica e financeira, que permitam aferir o retorno esperado e os riscos associados à implementação do modelo proposto.

Em termos mais amplos, este estudo pretende contribuir para o avanço do conhecimento na interseção entre inovação tecnológica, segurança digital e modelos de negócio digitais. Ao desenvolver e estruturar um modelo comercial centrado no utilizador, pretende-se demonstrar como a articulação entre tecnologia e estratégia empresarial pode ser orientada para a criação de valor, sustentabilidade e diferenciação competitiva no mercado global.

1.4 Abordagem Metodológica

A presente dissertação adota uma abordagem metodológica de natureza qualitativa, com o intuito de compreender, em profundidade, as perceções, motivações, expectativas e preocupações de potenciais utilizadores relativamente ao dispositivo KIS.

A natureza exploratória do estudo justifica-se pelo facto de o produto em análise ainda se encontrar numa fase conceptual e de desenvolvimento, o que torna essencial recolher perspetivas que orientem nas decisões quanto à funcionalidade do dispositivo, à proposta de valor e, sobretudo, à definição de um modelo de negócios viável e ajustado às exigências do mercado.

Neste contexto, optou-se pela utilização da metodologia de *Focus Group*, enquanto instrumento de validação e recolha de dados primários. Segundo o estudo realizado por David L Morgan (2021) esta metodologia, criada por Robert K. Merton na década de 1940, foi posteriormente refinada e amplamente aplicada em estudos de mercado, inovação e ciências sociais.

A sua principal mais-valia reside na possibilidade de gerar dados valiosos através da interação entre os participantes, que permitirá aceder a um nível de profundidade e espontaneidade frequentemente inacessível por via de métodos puramente quantitativos ou entrevistas individuais.

O Focus Group será estruturado com base num guião de discussão previamente elaborado, composto por questões abertas e orientadoras, com o objetivo de recolher perceções qualitativas relevantes para a validação da proposta de valor e do modelo de negócio do dispositivo KIS.

Para além da avaliação da relevância percebida das funcionalidades principais do produto e da recolha de sugestões para possíveis melhorias, a sessão incidirá especificamente sobre os nove elementos do *Business Model Canvas*.

Serão analisadas, de forma estruturada, as perceções dos participantes relativamente à proposta de valor do KIS, aos segmentos de clientes a que se dirige, aos canais de distribuição mais adequados, à natureza do relacionamento com os clientes, às fontes de receita, aos recursos-chave necessários, às atividades-chave a desenvolver, aos parceiros estratégicos a envolver e, finalmente, à estrutura de custos associada à produção e comercialização da solução.

Contudo, é importante referir que os valores presentes para o exercício de estrutura de custos e receitas são meramente especulativos dado que este projeto se insere no âmbito de uma dissertação de Mestrado e por esse motivo os valores presentes no plano de negócios são meramente especulativos, uma vez que para maior rigor seria necessário um desenvolvimento mais avançado do projeto e orçamentos reais, mas foi reafirmada a importância de uma abordagem concisa para garantir a sustentabilidade durante o processo de validação comercial e industrialização do produto).

Esta abordagem permitirá não só analisar a adequação estratégica do modelo de negócio delineado, como também recolher contributos empíricos que sustentem a sua afinação e adaptação às exigências reais do mercado.

Participaram nas sessões quatro Professores Doutores do Instituto Superior de Contabilidade e Administração do Porto (ISCAP), todos com experiência profissional e académica relevante, o que lhes confere um conhecimento aprofundado da realidade empresarial e uma abordagem aplicada aos temas que foram sujeitos a análise e validação.

O Professor Doutor José Agostinho de Sousa Pinto, orientador da presente dissertação, é Professor Coordenador na área de Sistemas de Informação e Vice-Presidente do ISCAP para a área da Transformação Organizacional, Investigação e Inovação Pedagógica. Doutorado em Engenharia de Tecnologias e Sistemas de Informação pela Universidade do Minho, desenvolveu também atividade como gestor de tecnologias e sistemas de informação em grandes grupos económicos.

Coordena o Mestrado de Negócio Eletrónico, é investigador integrado do CEOS.PP e tem produzido investigações relevantes nas áreas de gestão do conhecimento, serviços partilhados e comércio eletrónico, o que articula o seu percurso académico com uma forte ligação à realidade empresarial e à inovação tecnológica.

O Professor Doutor Pedro Mendonça da Silva é Professor Adjunto na área de Gestão e Diretor do Mestrado de Marketing Digital. Para além da sua atividade académica, conta com uma vasta carreira de quase duas décadas como consultor independente de gestão estratégica, marketing e internacionalização de negócios. Desempenhou funções de direção comercial em várias empresas e liderou projetos ligados à organização de grandes eventos empresariais e feiras internacionais, com forte componente tecnológica e digital.

A sua experiência prática em desenvolvimento e validação de modelos de negócio em diversos setores económicos, aliada à sua produção académica sobre a transformação digital e inovação, tornam o seu contributo particularmente relevante para dissertações centradas em soluções tecnológicas aplicadas ao mercado.

O Professor Doutor Rui Humberto Ribeiro Pereira possui licenciatura em Engenharia Eletrotécnica e de Computadores, Mestrado em Tecnologia Multimédia e Doutoramento em Sistemas e Software. A sua atividade académica está fortemente ligada às áreas da programação orientada a objetos, linguagens de marcação, interfaces digitais, virtualização e serviços web, o que são competências fundamentais para o desenvolvimento de soluções tecnológicas orientadas ao utilizador.

Para além da sua vertente científica, o seu conhecimento técnico aplicado ao design de software e arquitetura de sistemas reforça a capacidade de análise de propostas que, como a presente dissertação, cruzam inovação tecnológica e viabilidade de mercado.

O Professor Doutor Luís António Rodrigues é Professor Adjunto na área de Sistemas de Informação, com especialização em Gestão de Sistemas de Informação e “*Business Process Management*” (Gestão de Processos de Negócio). A sua experiência académica é complementada pela investigação aplicada em modelos de negócio baseados em tecnologias de informação, o que se traduz numa visão crítica sobre a estruturação e avaliação de propostas empresariais sustentadas em soluções digitais. A sua competência em metodologias de investigação, aliada ao conhecimento prático da integração de processos tecnológicos em contextos organizacionais, acrescenta rigor à análise metodológica e estratégica desenvolvida ao longo desta dissertação.

Esta diversidade de perfis visa garantir uma apreciação abrangente e fundamentada do modelo de negócios proposto para o KIS, o que permitiu analisá-lo não apenas sob a perspetiva tecnológica, mas também nas suas dimensões estratégicas, operacionais e metodológicas.

A combinação de experiência académica e prática dos participantes contribuirá para uma avaliação crítica e realista da viabilidade e potencial de implementação da proposta no mercado.

A moderação do *Focus Group* será conduzida pelo autor da dissertação, Omar Soares, em conjunto com o Professor Doutor José Agostinho de Sousa Pinto, com o objetivo de assegurar a fluidez e equilíbrio na participação dos intervenientes, e a qualidade dos dados recolhidos para análise posterior.

Em suma, a metodologia adotada nesta investigação pretende articular a análise qualitativa das perceções do mercado com a modelação estratégica e financeira do projeto, de forma a permitir responder de forma fundamentada à questão central da dissertação: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?”

1.5 Estrutura do Documento

A presente dissertação encontra-se estruturada em cinco capítulos principais, seguidos pelas referências bibliográficas, apêndices e anexos, de forma a proporcionar uma leitura lógica, progressiva e coerente do percurso de investigação desenvolvido.

O Capítulo de Introdução apresenta de forma sucinta o tema da investigação, a sua relevância no contexto atual da segurança digital e uma visão geral sobre a problemática de estudo, de forma a servir de ponto de partida para a compreensão global do trabalho.

O Capítulo I – Enquadramento da Investigação contextualiza o projeto, ao expor o enquadramento teórico e prático da proposta, a motivação subjacente à escolha do tema, o desafio identificado e os objetivos traçados. Inclui ainda a descrição da abordagem metodológica adotada onde se apresenta a estrutura geral da dissertação.

O Capítulo II – Estado da Arte corresponde à revisão de literatura, onde são analisados os principais conceitos, modelos e estudos relevantes para a temática em estudo. São abordados tópicos como o Business Model Canvas, a metodologia Focus Group, a problemática da gestão de palavras-passe, os mecanismos de proteção biométrica, as carteiras digitais físicas e os princípios de segurança e privacidade de dados.

O Capítulo III – Abordagem Metodológica descreve em detalhe a metodologia de investigação utilizada, clarifica a questão da investigação, os objetivos gerais e específicos e a justificação da escolha da metodologia qualitativa, com destaque para a aplicação da técnica de *Focus Group* como instrumento de discussão e validação de dados.

O Capítulo IV – Focus Group apresenta a estrutura do plano de negócios concebido para o dispositivo KIS, detalha a preparação e realização do Focus Group com especialistas, expõe os resultados obtidos e discute os ajustes e decisões estratégicas decorrentes da validação empírica do modelo de negócio.

O Capítulo V – Conclusão sintetiza os principais contributos do estudo e da metodologia aplicada, reflete sobre os objetivos inicialmente propostos e os resultados alcançados. É ainda apresentada uma análise crítica das dificuldades e limitações encontradas ao longo do processo de investigação, bem como a definição de trabalhos futuros que visam a continuidade e o desenvolvimento do projeto.

O documento termina com a listagem das referências bibliográficas utilizadas ao longo da investigação, o apêndice no qual se encontra o plano de negócios estruturado para o KIS e atualizado com base nos dados recolhidos no Focus Group e o anexo, na qual inclui, o guião utilizado na realização do *Focus Group*.

A presente dissertação tem como objetivo responder à questão: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?”, com foco principal a estruturação e desenvolvimento de um modelo de negócio viável, escalável e orientado para o mercado.

A crescente digitalização da vida pessoal e profissional, acelerada pelas exigências de mobilidade, segurança e conectividade, tem tornado cada vez mais evidentes as limitações dos modelos tradicionais de proteção digital. O aumento dos ciberataques, a fragilidade das palavras-passe, a complexidade da gestão de identidades e o risco associado ao armazenamento de criptoativos criam uma oportunidade clara para soluções integradas. Contudo, conforme constatado por Murray e Scuotto (2015), o sucesso de uma inovação tecnológica não depende exclusivamente da sua capacidade funcional ou do avanço técnico, mas sim da sua inserção estratégica num modelo de negócio que permita gerar, entregar e capturar valor de forma sustentável.

Neste contexto, o dispositivo KIS é concebido como um artefacto multifuncional de segurança digital, mas a sua proposta de valor só ganha relevância prática quando estruturada dentro de um modelo de negócio coerente e devidamente estruturado.

Para esse fim, será utilizado o *Business Model Canvas* como ferramenta central de desenvolvimento e estruturação, ao permitir decompor a proposta em nove elementos fundamentais: a proposta de valor, segmentos de clientes, canais, relacionamento com clientes, fontes de receita, recursos-chave, atividades-chave, parceiros estratégicos e estrutura de custos.

A escolha desta ferramenta justifica-se pela sua ampla adoção em contextos de inovação tecnológica, especialmente em produtos orientados ao consumidor final e a soluções empresariais integradas. Para além da estruturação conceptual do modelo de negócio, a análise qualitativa será realizada através da aplicação da metodologia de *Focus Group*, pela sua relevância na recolha de perceções qualitativas sobre propostas de valor e modelos de negócio em fase de desenvolvimento.

As questões formuladas incidem diretamente sobre os nove elementos do *Business Model Canvas*, ao permitir analisar a perceção dos participantes relativamente ao plano de negócios estruturado. Paralelamente, será avaliada a relevância percebida das funcionalidades do dispositivo KIS, bem como eventuais sugestões de melhoria.

Esta abordagem permitirá não apenas analisar os pressupostos estratégicos definidos, mas também identificar desenvolvimentos necessários à adequação da solução.

Neste enquadramento, o dispositivo não é considerado apenas um fim isolado, mas como o elemento central de uma plataforma estratégica de segurança digital, cuja viabilidade dependerá da coerência entre os seus atributos técnicos, as exigências do mercado, a clareza do seu posicionamento comercial e da sua capacidade de gerar e capturar valor de forma sustentável.

Assim, o presente estado da arte e revisão de literatura tem por base duas premissas essenciais, primeiro, que a segurança digital exige soluções integradas, fiáveis e adaptadas a diferentes contextos de utilização, segundo, que a transformação de uma solução técnica em produto viável depende de um modelo de negócio bem estruturado e sustentável. É nesta interseção entre tecnologia e gestão estratégica que se posiciona o KIS.

2 Revisão de literatura

2.1 Business Model Canvas

O Business Model Canvas (BMC) é uma ferramenta conceptual desenvolvida por Osterwalder e Pigneur (2010) com o propósito de representar visualmente a lógica de criação, entrega e captura de valor por parte de uma organização.

A escolha do Business Model Canvas (BMC) como estrutura conceptual para o desenvolvimento do modelo de negócio do dispositivo KIS assenta na sua eficácia enquanto ferramenta estratégica de representação visual e sintética da lógica de criação, entrega e captura de valor. Desenvolvido por Osterwalder e Pigneur (2010), o BMC tem-se consolidado como uma referência em contextos de inovação tecnológica e empreendedorismo digital, pela sua capacidade de integrar as nove dimensões essenciais do modelo de negócios num quadro dinâmico e adaptável. Ao contrário de modelos mais tradicionais, como o plano de negócios clássico linear ou o modelo SWOT, o BMC permite não só estruturar uma proposta estratégica, mas também promover a iteração, experiência e validação progressiva, características indispensáveis em projetos emergentes e tecnologicamente orientados como o KIS.

No entanto, reconhece-se que o BMC possui limitações, designadamente o seu carácter descritivo e a ausência de uma orientação prescritiva clara, conforme apontado por Becker e Bröcker (2021). Em contraste, modelos como o Balanced Scorecard introduzem métricas de desempenho e alinhamento estratégico mais eficazes, embora menos adaptáveis na fase inicial de ideação. Do mesmo modo, abordagens como a Lean Startup privilegiam a iteração rápida e a retroalimentação contínua, mas carecem de uma estrutura formal do modelo de negócio.

O BMC surge, assim, como uma solução intermédia adequada, ao conjugar a profundidade estratégica com a flexibilidade metodológica, sendo particularmente eficaz quando complementado com métodos qualitativos como o Focus Group.

Paralelamente, a adoção da estrutura do plano de negócios proposta pelo IAPMEI – “Como Elaborar um Plano de Negócios – Guia Explicativo” – decorre da sua qualidade e eficácia prática, do alinhamento com o ecossistema empresarial português e da sua orientação clara para a análise económico-financeira. Comparativamente a modelos internacionais, como o proposto pelo Small Business Administration, o guia do IAPMEI destaca-se por responder às exigências de financiamento, apoio institucional e apresentação a possíveis acionistas nacionais, tornando-o uma escolha estrategicamente fundamentada neste contexto.

A sua adoção generalizada em ambientes de inovação, *startups* e projetos de base tecnológica deve-se à sua capacidade de simplificar a estrutura estratégica sem descuidar a complexidade estrutural das operações empresariais.

Segundo Murray e Scuotto (2015), o *Business Model Canvas* constitui uma abordagem altamente eficaz para transformar ideias em propostas de valor viáveis. Os autores argumentam que, num contexto marcado por elevada incerteza, como os setores da inovação tecnológica e da cibersegurança, o *Business Model Canvas* permite validar hipóteses estratégicas de forma eficaz.

No seu estudo “*The Business Model Canvas*” (2015), estes detalham como os nove elementos do Modelo Canvas se completam para gerar coerência organizacional, na qual destacam a importância da proposta de valor como elemento central, a partir do qual todos os restantes elementos devem ser ajustados.

A pesquisa dos autores baseia-se na análise prática da aplicação do *Business Model Canvas* em projetos empreendedores, e demonstram que este modelo contribui significativamente para alinhar as diferentes áreas funcionais de uma organização e para tornar o processo de decisão mais transparente. Os autores destacam ainda que a linguagem visual e a estrutura sintética do Modelo Canvas favorecem o diálogo entre fundadores, investidores e utilizadores finais, ao promover a criação de soluções mais centradas e adaptadas ao mercado. Em projetos como o KIS, esta característica é essencial para integrar perspetivas técnicas, comerciais e comportamentais num modelo de negócio coerente e sustentável.

O modelo está estruturado em nove elementos fundamentais que, de forma interdependente, descrevem a arquitetura organizacional de qualquer empresa:

1. Proposta de Valor – define o conjunto de produtos e serviços que criam valor para um segmento de clientes específico, que respondem a necessidades explícitas ou latentes;

2. Segmentos de Clientes – identifica os grupos-alvo que a empresa pretende servir, com base nas características demográficas, comportamentais, ou necessidades específicas;

3. Canais – descreve os meios pelos quais a empresa comunica e entrega a proposta de valor aos clientes;

4. Relacionamento com Clientes – especifica o tipo de relacionamento que a organização estabelece com os diferentes segmentos de clientes, desde o atendimento personalizado até ao automatizado;

5. Fontes de Receita – identifica a forma como a empresa gera rendimento a partir de cada segmento, que inclui venda direta, subscrição, licenciamento, entre outros modelos;

6. Recursos-Chave – refere-se aos ativos estratégicos necessários para criar e oferecer a proposta de valor, alcançar mercados e manter a relação com os clientes;

7. Atividades-Chave – engloba os processos e operações essenciais para que o modelo de negócio funcione, como produção, marketing ou desenvolvimento tecnológico;

8. Parcerias Estratégicas – contempla a rede de fornecedores, parceiros e/ou alianças necessárias para potencializar os recursos, reduzir riscos ou aceder a novas competências;

9. Estrutura de Custos – apresenta os custos mais relevantes e inerentes à execução do modelo, na qual distingue os custos fixos, variáveis, de escala ou âmbito.

Já Becker e Bröcker (2021) propõem uma análise crítica mais aprofundada das vantagens e limitações do *Business Model Canvas*, com base numa revisão sistemática da literatura e na observação de casos práticos.

Os autores reconhecem que o Modelo Canvas se consolidou como uma ferramenta de referência na inovação empresarial, sobretudo pela sua capacidade de representar graficamente a lógica do negócio de forma concisa, ao facilitar a comunicação entre as equipas e a experimentação estratégica.

No entanto, na sua análise identificam também limitações estruturais e epistemológicas do modelo. Uma das principais críticas refere-se à natureza descritiva do *Business Model Canvas*, que carece de uma orientação prescritiva clara, ou seja, o modelo demonstra o que existe, mas não necessariamente o que deve ser feito. Além disso, Becker e Bröcker argumentam que este modelo não contempla fatores externos críticos, como a concorrência, o enquadramento legal, ou os aspetos culturais e institucionais dos mercados.

A ausência destes elementos pode limitar a sua aplicação em mercados complexos ou regulados, como é o caso dos produtos tecnológicos que envolvem dados sensíveis, autenticação biométrica e ativos financeiros digitais.

Apesar dessas reservas, os autores concluem que o Modelo Canvas continua a ser uma ferramenta valiosa quando complementada com métodos de análise qualitativa e de apoio à decisão, nomeadamente *benchmarking*, prototipagem de modelos e grupos focais.

Neste sentido, a presente dissertação integra o *Business Model Canvas* como estrutura de base, complementada por uma metodologia qualitativa (*Focus Group*), de forma a colmatar estas limitações e obter uma compreensão mais profunda da viabilidade comercial da proposta KIS.

2.2 Metodologia *Focus Group*

A metodologia de *Focus Group* tem se demonstrado como uma das abordagens qualitativas mais eficazes na validação e recolha de dados em investigação social, organizacional e de mercado. A sua essência reside na obtenção de conhecimento coletivo através da interação entre os participantes, conduzida num ambiente controlado, mas flexível, com o objetivo de aceder a perceções, experiências e atitudes de forma aprofundada.

De acordo com Lane et al. (2001), os *Focus Groups* permitem captar significados subjetivos e interpretações sociais que dificilmente seriam compreendidas através de métodos quantitativos. A investigação qualitativa beneficia, assim, da espontaneidade das respostas e da construção coletiva do discurso, fatores que conferem riqueza e densidade analítica aos dados recolhidos. Os autores enfatizam que o sucesso da técnica depende da clareza dos objetivos, da estruturação rigorosa do guião e da competência do moderador na gestão do grupo e do tempo.

Para complementar essa perspetiva, o estudo de Ning et al. (2024) destaca a importância de fatores situacionais que são frequentemente negligenciados nos estudos empíricos com recurso à metodologia *Focus Group*:

1. Elementos relacionais: Refere-se à forma como os participantes interagem entre si durante a discussão. A dinâmica do grupo, inclusive as normas sociais, relações de poder e estilos de comunicação, pode afetar a profundidade e a qualidade das informações compartilhadas.

Por exemplo, a presença de indivíduos dominantes pode inibir a participação de outros membros, enquanto um ambiente colaborativo pode incentivar uma troca mais eficiente de ideias.

2. Características dos Participantes: Inclui fatores como o gênero, estatuto socioeconómico, experiências anteriores e literacia. Estas características podem influenciar as perceções e atitudes dos participantes e afetar a forma como contribuem para a discussão.

3. Influência do Moderador: O estilo de moderação, a formulação de perguntas, intervenções e comportamentos não verbais, pode direcionar ou restringir a discussão. Moderadores que não mantêm uma postura neutra podem, inadvertidamente, conduzir os participantes a respostas específicas ou desencorajar a expressão aberta de opiniões divergentes.

Os autores defendem que aspetos como o espaço físico, a composição do grupo, a linguagem utilizada e a dinâmica relacional entre os participantes influenciam significativamente a qualidade da informação obtida. Este contributo é particularmente relevante para contextos académicos e empresariais, nos quais o ambiente deve ser estrategicamente moldado para favorecer a expressão livre e crítica dos participantes.

Mwilongo (2025) acrescenta à revisão um conjunto de boas práticas operacionais, organizadas sob a forma de "*dos and don'ts*" na condução desta metodologia. Entre as recomendações destacam-se os critérios de seleção dos participantes, o uso de perguntas abertas, a neutralidade do moderador e a necessidade de evitar enviesamentos pela liderança do grupo ou pela incorreta formulação das questões. Estes princípios suportam a orientação da fiabilidade e validade dos dados obtidos e asseguram que as ilações retiradas possam ser consideradas representativas e aplicáveis ao objeto de estudo.

A origem epistemológica da técnica remonta a Robert K. Merton, reconhecido como o seu criador formal, tal como analisado por Morgan (2021). Este autor sublinha a intenção original de Merton de aliar a interação social à investigação empírica sistemática, sobretudo em estudos de comunicação de massa e perceção pública. A abordagem clássica de Merton defendia a combinação da liberdade de expressão com direção temática rigorosa, uma metodologia que permanece atual e pertinente, especialmente em investigações com objetivos de validação estratégica, como é o caso desta dissertação.

Deste modo, a presente investigação recorre ao *Focus Group* enquanto técnica de validação do modelo de negócio do KIS, através do desenvolvimento de um guião com base nos nove elementos do *Business Model Canvas*. Os participantes foram selecionados com base em critérios de competência técnica e diversidade académica, e a moderação será conduzida pelo autor da dissertação Omar Soares, em articulação com o orientador desta dissertação, Professor Doutor José Agostinho de Sousa Pinto.

Esta abordagem visa assegurar a recolha de informações fiáveis e suscetíveis de gerar conclusões teóricas relevantes, que respeitem os princípios metodológicos identificados na literatura especializada.

2.3 Memorização de Palavras-passe

A dificuldade em criar e memorizar palavras-passe seguras constitui um dos principais obstáculos à atual segurança digital e constitui implicações diretas na adoção de práticas inadequadas por parte dos utilizadores. A dependência excessiva deste mecanismo de autenticação, associado à complexidade crescente das exigências de combinações (de letras, números e símbolos), tem contribuído para um fenómeno generalizado de fadiga cognitiva, que resulta em comportamentos de risco e baixa eficácia das estratégias de cibersegurança.

O estudo de Tanni et al. (2022), foca-se na perceção dos utilizadores relativamente às suas práticas de gestão de palavras-passe. Os dados recolhidos revelam que uma elevada proporção dos inquiridos reutiliza as mesmas credenciais em múltiplas plataformas, na qual muitas vezes se baseiam em dados pessoais facilmente dedutíveis, como nomes de familiares, aniversários ou sequências numéricas simples. Esta prática resulta da conjugação de dois fatores: por um lado, a perceção errada do risco associado ao uso pessoal de serviços online, por outro, a incapacidade prática de memorizar múltiplas palavras-passe seguras, dada a sua complexidade e volume. Os autores evidenciam ainda que, mesmo após ações de sensibilização, a maioria dos utilizadores mantém práticas inseguras e optam pela conveniência em detrimento da segurança.

Em complemento a esta análise, a investigação de Fernando, Dissanayake, Dushmantha e Liyanage (2023), oferece uma revisão sistemática sobre os desafios e limitações das soluções atuais de gestão de palavras-passe. Os autores observam que, apesar da existência de tecnologias como gestores de palavras-passe e autenticação multifator, a adoção destas ferramentas permanece limitada. Muitos utilizadores demonstram desconfiança quanto à segurança dos próprios gestores de senhas e expressam reservas quanto à centralização de credenciais num único ponto de falha.

Além disso, há um défice de competências na configuração e utilização adequada dessas soluções, o que compromete a sua eficácia.

O estudo conclui que a persistência do fator humano como elo mais fraco da cadeia de segurança torna urgente a transição para métodos alternativos de autenticação que sejam simultaneamente seguros, intuitivos e transparentes para o utilizador final.

Por sua vez, Altarawneh et al. (2025), analisam os níveis de literacia digital entre os estudantes do ensino secundário, revelando uma preocupante lacuna de conhecimento sobre práticas básicas de cibersegurança, como a criação e gestão de palavras-passe. Os dados indicam que a maioria dos estudantes utiliza combinações simples e repete as mesmas senhas em várias contas, frequentemente armazenando-as em ferramentas inseguras (como blocos de notas ou browsers). O estudo evidencia ainda que a sensibilização institucional sobre boas práticas de segurança é insuficiente ou ineficaz, o que leva os jovens a desenvolver hábitos informais e vulneráveis desde cedo.

Em síntese, a literatura aponta para uma problemática recorrente e transversal a diferentes perfis sociodemográficos: a memorização de palavras-passe representa uma sobrecarga cognitiva significativa, à qual os utilizadores respondem com práticas compensatórias inseguras e ineficazes. Esta realidade compromete a integridade dos sistemas de autenticação tradicionais e reforça a necessidade de adoção de alternativas mais seguras, práticas e fiáveis, como a autenticação biométrica.

A proposta de valor do dispositivo KIS responde diretamente a essa problemática ao eliminar a necessidade de memorizar inúmeras credenciais, através da integração de mecanismos biométricos de autenticação. Esta abordagem reduz o fator de erro humano e melhora substancialmente a segurança e a experiência do utilizador, estando, assim, alinhada com as conclusões evidenciadas nos estudos analisados.

2.4 Proteção por Biometria

A autenticação biométrica tem-se consolidado como uma das formas mais promissoras e seguras de validação da identidade digital, sobretudo em contextos onde se procura eliminar o risco associado às palavras-passe e reduzir a vulnerabilidade dos sistemas a ataques externos. A biometria baseia-se em características físicas ou comportamentais únicas de cada indivíduo, como impressões digitais, traços faciais, padrões de íris, voz ou até comportamento gestual e asseguram um método de autenticação intransferível, permanente e altamente individualizado.

O estudo de Balamurugan (2024), apresenta uma análise crítica desta tecnologia, ao expor simultaneamente os seus pontos fortes e os riscos subjacentes. O autor argumenta que a biometria representa uma evolução significativa face aos sistemas baseados em conhecimento (palavras-passe) ou posse (tokens), dado que elimina o risco de esquecimento, perda ou partilha indevida de credenciais. O estudo evidencia que os sistemas biométricos são intrinsecamente mais resistentes a ataques de *phishing*, *keylogging* ou *brute force*, uma vez que não envolvem dados transferíveis por meios digitais tradicionais.

Contudo, o autor alerta para uma característica crítica da biometria, a sua irreversibilidade. Se uma impressão digital for comprometida, esta não pode ser alterada como se faz com uma senha convencional. Isto torna os sistemas biométricos particularmente sensíveis a falhas na arquitetura de proteção dos dados recolhidos.

O artigo destaca ainda a importância de aplicar políticas rigorosas de segurança, tais como armazenamento local encriptado (em vez de bases de dados centrais) e controlo sobre a forma como os dados biométricos são recolhidos, tratados e destruídos. Por fim, o autor enfatiza que a aceitação dos utilizadores depende da confiança na privacidade, o que exige transparência tecnológica e conformidade com normativas como o RGPD.

Por outro lado, Sheikh (2025), adota uma perspetiva evolutiva e integrada sobre a tecnologia biométrica, ao destacar os seus benefícios operacionais e a sua aplicação crescente em sectores como a banca, saúde, segurança pública e tecnologia de consumo.

O autor documenta a trajetória da autenticação biométrica desde os seus primeiros usos em ambientes governamentais e militares até à sua incorporação em dispositivos pessoais, como telemóveis e carteiras digitais. Segundo o autor, o principal contributo da biometria reside na sua capacidade de melhorar simultaneamente a segurança e a experiência do utilizador, ao reduzir o atrito no processo de autenticação e proporcionar um acesso contínuo, rápido e personalizado.

O estudo salienta que os sistemas biométricos modernos, quando associados a dispositivos físicos, minimizam a exposição a redes externas e a vulnerabilidades sistemáticas. Sheikh (2025) defende ainda que a biometria, ao permitir a autenticação contínua, pode ser integrada em estratégias dinâmicas de gestão de identidade, com aplicações eficazes em ambientes corporativos e plataformas financeiras.

No entanto, o autor também reitera que a biometria deve ser tratada como parte de um ecossistema de segurança mais amplo, onde coexistem técnicas complementares, como a encriptação de dados, segmentação de permissões e monitorização de atividade anómala.

A análise destes dois estudos permite concluir que a proteção por biometria oferece benefícios claros em termos de fiabilidade, uso e resistência a ameaças externas, mas requer uma estruturação de segurança adequada para evitar riscos associados à centralização e reutilização dos dados biométricos.

No âmbito do projeto KIS, a utilização da autenticação exclusivamente biométrica visa precisamente resolver os problemas associados à gestão de palavras-passe, ao oferecer ao mesmo tempo uma solução efetiva e centrada no utilizador. Os dados biométricos serão processados e armazenados localmente, no próprio dispositivo, de forma a minimizar o risco de intrusão ou roubo de identidade. Esta abordagem está em linha com as melhores práticas sugeridas pela literatura científica e contribui para o posicionamento do KIS como uma resposta tecnológica moderna, segura e eficiente.

2.5 Proteger criptoativos em “cold wallets”

A proteção de criptoativos representa um desafio crescente no ecossistema digital, uma vez que estas ativos digitais operam de forma descentralizada e, por norma, sem intermediários institucionais. O armazenamento seguro de chaves privadas é, portanto, um requisito crítico para a integridade e acessibilidade dos ativos.

As designadas “cold wallets”, constituem uma das soluções mais seguras para a gestão de criptoativos, uma vez que se tratam de dispositivos físicos e/ou sistemas offline que mantêm os dados de acesso fora da rede, que os protegem de ameaças digitais ativas.

O estudo de Kirobo (2025), apresenta uma revisão abrangente das vulnerabilidades associadas às carteiras digitais. O autor identifica que as “hot wallets” (soluções ligadas permanentemente à internet) são particularmente vulneráveis a ataques de *malware*, *phishing*, engenharia social e exploração de falhas em APIs (conjuntos de regras, protocolos e definições que permitem que diferentes sistemas, aplicações ou serviços comuniquem entre si de forma estruturada e segura).

As perdas resultantes de falhas de segurança neste tipo de carteiras (*“hot wallets”*) são amplamente documentadas e frequentemente irreversíveis.

Em contrapartida, as *“cold wallets”* demonstram uma resiliência significativamente superior, ao reduzirem a superfície de ataque e eliminarem a dependência de conectividade contínua. O estudo salienta ainda que a ausência de ligação em tempo real suporta o impedimento ao acesso remoto malicioso e torna extremamente difícil a extração das chaves privadas destes criptoativos.

Para complementar esta perspectiva, o estudo de Haryadi, et al. (2023), compara os diferentes modelos de carteiras (hot, cold e híbridas) com base em critérios de segurança, utilização e escalabilidade. Os autores concluem que, embora as *“hot wallets”* ofereçam conveniência e acessibilidade imediata, as *“cold wallets”* representam a solução mais segura para armazenar grandes quantidades de ativos ou ativos de elevado valor. O estudo destaca que estas suportam a eliminar vulnerabilidades de acesso não autorizado, ataques por canal lateral e dependência de terceiros. Contudo, aponta também algumas limitações em termos de experiência do utilizador, nomeadamente no que respeita à necessidade de hardware dedicado, à gestão física do dispositivo e ao risco de perda do mesmo sem cópia de segurança.

Os autores defendem, portanto, uma abordagem integrada, na qual *“cold wallets”* são utilizadas para o armazenamento a longo prazo (*“holding”*) e *“hot wallets”* apenas para operações pontuais ou de baixo valor (*“liquidez operativa”*). Este modelo é considerado ideal para ambientes empresariais e institucionais que exigem um compromisso entre segurança e funcionalidade.

No âmbito do projeto KIS, a integração de uma componente de *“cold wallet”* representa uma resposta direta à necessidade de proteção eficaz de criptoativos, ao proporcionar aos utilizadores a possibilidade de armazenar localmente os seus ativos digitais num ambiente isolado e sem dependência de redes externas.

Esta arquitetura, aliada à autenticação biométrica e sistema de *“backup”*, cria um artefacto de segurança multicamada, resistente a ataques remotos e orientado para a proteção de ativos digitais de elevado valor. A escolha de *“cold wallet”* justifica-se, assim, com base nos princípios da segurança da informação (confidencialidade, integridade e disponibilidade) e está alinhada com as boas práticas descritas na literatura científica analisada.

2.6 Segurança e Privacidade de Dados

Com o crescente aumento da digitalização de dados pessoais, comerciais e administrativos, a segurança e a privacidade dos dados emergem como pilares críticos da segurança digital. A exposição crescente a ameaças virtuais, a recolha em massa de dados pessoais pelas empresas e a fragmentação reguladora internacional tornam urgente a consolidação de mecanismos técnicos e comportamentais na proteção da informação.

No artigo de Gajjar (2024), este identifica três principais causas de vulnerabilidade: a complexidade tecnológica das infraestruturas digitais, o crescente desenvolvimento das ameaças e a disparidade entre os avanços tecnológicos e as práticas dos utilizadores. O autor enfatiza que tecnologias como encriptação homomórfica, privacidade diferencial, *blockchain* e a inteligência artificial aplicada à segurança virtual têm potencial para mitigar riscos de forma significativa, desde que integradas num ecossistema digital coerente e orientado para a prevenção. Contudo, Gajjar adverte que tais tecnologias por si só não garantem proteção efetiva se não forem acompanhadas de políticas sólidas de gestão de dados e de medidas de sensibilização junto dos utilizadores. A proteção de dados deve ser vista, segundo o autor, como uma função transversal à arquitetura digital, e não como uma camada adicional aplicada a posteriori.

Já o estudo de Santos e Pinto (2025), aprofunda a componente psicológica e cognitiva da problemática, ao analisar como os indivíduos percecionam e reagem às ameaças da sua privacidade. Através de uma abordagem empírica e multidisciplinar, os autores demonstram que a adoção de comportamentos seguros não depende exclusivamente da consciência do risco, mas também de fatores como a familiaridade com o sistema, a utilização da solução e a confiança depositada nas entidades responsáveis pelo seu funcionamento.

O estudo conclui que existe uma discrepância significativa entre o conhecimento teórico sobre as boas práticas de segurança e a sua aplicação prática, motivada por heurísticas cognitivas que privilegiam a conveniência imediata em detrimento da proteção a longo prazo. A investigação sublinha a importância de desenvolver soluções que minimizem a carga cognitiva do utilizador e que ofereçam segurança sem comprometer a fluidez da experiência digital.

Complementarmente, Kaiser (2016) analisa, numa perspetiva sociológica, como diferentes grupos etários percecionam e priorizam a privacidade online.

Os resultados indicam que os utilizadores mais jovens, embora sejam mais experientes em ambientes digitais, demonstram uma maior tolerância ao monitoramento e partilha de dados pessoais, frequentemente em troca de acesso gratuito ou personalizado a serviços.

Por contraste, os utilizadores mais velhos tendem a manifestar maior preocupação com a segurança, mas revelam menor capacidade para compreender ou utilizar mecanismos de proteção complexos. Esta variação etária exige, segundo Kaiser, uma adaptação dos sistemas de proteção às características do público-alvo, quer ao nível da comunicação, quer da utilização das ferramentas de privacidade.

A análise cruzada destes três estudos permite concluir que a segurança e a privacidade de dados online são desafios de natureza híbrida (tecnológica, comportamental e regulatória). As soluções eficazes devem incorporar mecanismos avançados de proteção técnica, mas também conseguir responder às limitações cognitivas e às preferências comportamentais dos utilizadores.

No âmbito do dispositivo KIS, estas recomendações são operacionalizadas através de uma abordagem integrada: os dados sensíveis (como a biometria) são guardados exclusivamente no próprio dispositivo, sem conexão a bases de dados externas.

O acesso é realizado por autenticação biométrica local, sem necessidade de memorizar ou transmitir palavras-passe e o design do sistema privilegia a simplicidade operacional sem comprometer a segurança. Esta proposta responde às exigências atuais da proteção de dados, conforme identificadas pela literatura, e reforça o valor estratégico do KIS enquanto solução de confiança num ecossistema digital cada vez mais vulnerável.

2.7 Palavras-passe seguras

Apesar das fragilidades associadas ao uso de palavras-passe, estas continuam a ser um dos mecanismos mais utilizados para autenticação digital. A importância de ter palavras-passe fortes, únicas e atualizadas é tornou-se empírica, contudo, a sua aplicação prática permanece um desafio para a maioria dos utilizadores.

O estudo de Master (2022), explora precisamente esta lacuna entre a recomendação e o comportamento, ao propor os gestores de palavras-passe como uma solução viável para simplificar e reforçar a segurança digital.

O autor argumenta que a maior parte dos utilizadores continua a adotar estratégias inseguras (como reutilizar acessos, optar por palavras-passe previsíveis ou anotá-las em locais acessíveis) devido à sobrecarga cognitiva associada à sua memorização.

O estudo demonstra que os gestores de palavras-passe não só permitem a criação e o armazenamento de credenciais de acesso eficazes e únicas para cada plataforma, como também automatizam o preenchimento dos campos de acesso e alertam para possíveis violações de segurança. Além disso, estes promovem uma maior consistência no uso de boas práticas, ao libertar os utilizadores da responsabilidade de memorizar senhas complexas e ao proporcionar uma experiência de autenticação mais fácil. No entanto, Master (2022) também reconhece que a adoção generalizada destas ferramentas é dificultada pela falta de literacia digital, pela desconfiança em soluções centralizadas e pela perceção de complexidade associada à configuração inicial.

Neste enquadramento, embora os gestores de palavras-passe representem um avanço face ao modelo tradicional de autenticação manual, continuam a depender do comportamento ativo do utilizador e da sua disciplina em manter as ferramentas atualizadas e protegidas por autenticação multifator. Esta dependência humana constitui um ponto crítico de vulnerabilidade que pode ser explorado por agentes maliciosos.

No contexto do projeto KIS, esta problemática é abordada de forma estrutural: ao substituir as palavras-passe por autenticação biométrica local e ao eliminar a necessidade de guardar senhas em bases de dados ou serviços *cloud*, o dispositivo propõe uma rutura com o paradigma tradicional de autenticação. Ao fazê-lo, oferece não apenas maior segurança, mas também uma experiência mais intuitiva, ao reduzir significativamente os pontos de falha associados ao fator humano.

CAPÍTULO III – ABORDAGEM METODOLÓGICA

3 Abordagem metodológica

A definição da abordagem metodológica desta dissertação resulta da necessidade de articular dois domínios interdependentes: por um lado, o desenvolvimento de um artefacto tecnológico inovador (o dispositivo KIS) e, por outro, a conceção e validação do respetivo modelo de negócio, centrado na sua inserção no mercado e criação de valor sustentável. Dado que a aceitação de inovações tecnológicas não depende unicamente da sua eficácia técnica, mas também da respetiva adequação às necessidades e expectativas dos utilizadores e possíveis investidores, optou-se por uma estratégia metodológica “*Focus Group*” devido à sua lógica qualitativa e exploratória.

O presente capítulo visa descrever, a abordagem metodológica adotada na investigação, de forma a garantir a coerência entre o problema formulado, os objetivos definidos e os procedimentos aplicados para a recolha e análise de dados. Ao considerar a natureza do objeto de estudo (que conjuga a conceção de um artefacto tecnológico com a validação do respetivo modelo de negócio) optou-se por uma estratégia metodológica qualitativa, centrada na compreensão aprofundada das perceções e expectativas de potenciais utilizadores e especialistas de distintas áreas de especialização.

O modelo de negócio a ser analisado será estruturado com base modelo Canvas, o que irá permitir decompor a proposta em nove componentes fundamentais (proposta de valor, segmento de clientes, canais, relacionamento com os clientes, fontes de receita, estrutura de custos, recursos, atividades e parcerias-chave) de forma a orientar a discussão, avaliação e validação por parte dos participantes do *Focus Group*. Esta opção metodológica irá permitir captar perceções, motivações, expectativas e eventuais barreiras à adoção da solução proposta, o que contribuirá para a adequação do modelo de negócio ao contexto real de mercado.

3.1 Questão/Problema da Investigação

A presente investigação procura responder à seguinte questão central: “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?”, com foco na estruturação e validação do modelo de negócio que sustenta a sua viabilidade comercial e estratégica.

Apesar da crescente procura por soluções de segurança digital e gestão de criptoativos, muitas iniciativas falham devido à ausência de modelos de negócio adequados à sua proposta de valor, aos seus segmentos de clientes e às dinâmicas reais do mercado.

Este problema de investigação parte do pressuposto de que, para além da eficácia tecnológica e da inovação funcional do dispositivo KIS, a sua adoção no mercado dependerá fundamentalmente da construção de um modelo de negócios sustentável, credível e alinhado com as expectativas dos seus segmentos-alvo.

Desta forma, a investigação posiciona-se na intersecção entre a inovação tecnológica e a estratégia empresarial, ao procurar compreender quais são os elementos fundamentais que devem compor o modelo de negócio do KIS para que este seja sustentável, atrativo e escalável. A validação empírica da proposta de valor, das fontes de receita, dos canais de distribuição, dos recursos e atividades-chave, e das relações com clientes, constitui o núcleo da problemática a explorar nesta dissertação.

3.2 Objetivo da Investigação

O objetivo geral da presente investigação consiste em responder à questão “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?” através da conceção, estruturação e validação de um modelo de negócios sustentável para o respetivo dispositivo (KIS).

Este objetivo geral desdobra-se nos seguintes objetivos específicos:

- Estruturar o modelo de negócio do KIS com base no Business Model Canvas, através dos seus nove elementos fundamentais e a sua respetiva inter-relação.
- Explorar, à luz da literatura científica e das tendências de mercado, os fatores críticos para a adoção de dispositivos de segurança digital.
- Recolher e analisar perceções qualitativas de potenciais utilizadores e especialistas através da metodologia de *Focus Group*.
- Avaliar a adequação da proposta de valor do KIS aos segmentos-alvo identificados.
- Validar a coerência interna e a exequibilidade dos componentes do modelo de negócio.

- Identificar as barreiras à adoção e recomendações práticas para o aperfeiçoamento do modelo de negócio.

A prossecução destes objetivos visa contribuir para a construção de uma solução tecnológica com fundamento estratégico, alicerçada em evidência empírica e alinhada com as exigências do ecossistema digital em constante transformação.

3.3 Metodologia da Investigação

A metodologia adotada nesta investigação assume uma natureza qualitativa, de cariz de discussão e interpretativo, adequada à análise aprofundada de fenómenos complexos, como a articulação entre tecnologia e estratégia de negócio. Este tipo de abordagem permite aceder a perceções, interpretações e significados atribuídos pelos participantes a um fenómeno ainda emergente, a adoção de dispositivos multifuncionais de segurança digital com base num modelo de negócio sustentável. Nesse contexto, foi aplicada a metodologia de *Focus Group*, amplamente reconhecida como uma ferramenta eficaz na validação e recolha de dados qualitativos.

A metodologia de *Focus Group* tem origem nas investigações sociológicas de Robert K. Merton durante a década de 1940, que a utilizou como instrumento para compreender reações e atitudes em contextos de comunicação de massas (Morgan, 2021).

Desde então, esta técnica tem-se consolidado como uma abordagem de investigação qualitativa particularmente eficaz para aceder a discursos, perceções e representações sociais sobre temas complexos e multidimensionais.

De acordo com Lane et al. (2001), o Focus Group caracteriza-se pela interação estruturada entre um número reduzido de participantes, orientada por um moderador que estimula a discussão de um conjunto de tópicos previamente definidos. Esta interação grupal, ao contrário da entrevista individual, permite que as ideias dos participantes sejam debatidas, questionadas e aprofundadas em tempo real, o que enriquece a qualidade e diversidade dos dados recolhidos.

Nesta investigação, o Focus Group foi concebido como uma ferramenta para recolher contributos sobre a estruturação e validação da ideia e do modelo de negócio do KIS. Procurou-se garantir a validade metodológica e a riqueza do discurso através de uma configuração que respeita as recomendações avançadas por Mwilongo (2025),

nomeadamente: seleção criteriosa dos participantes, clareza na definição dos objetivos da sessão, equilíbrio na condução das intervenções e neutralidade do moderador.

Conforme defendido por Ning et al. (2024), os aspetos como o ambiente físico, o layout da sala, a linguagem adotada e a composição heterogénea do grupo são fatores cruciais que influenciam significativamente a profundidade e autenticidade das respostas obtidas. Neste contexto, foi assegurado um espaço reservado, confortável e informal para a realização das sessões, ao promover um ambiente propício à expressão livre, à escuta ativa e à participação equitativa entre os intervenientes.

A estratégia metodológica foi operacionalizada em duas sessões de Focus Group, conduzidas em momentos distintos, mas integradas num mesmo processo sequencial de investigação.

Os participantes foram selecionados com base em critérios de relevância e diversidade de conhecimento e experiência profissional, ao assegurar a presença de Professores Doutores com experiência comprovada nas áreas da gestão, segurança digital, inovação tecnológica e sistemas de informação. A composição do grupo garantiu a pluralidade de perspetivas e densidade argumentativa, critérios valorizados por Lane et al. (2001) e reiterados por Mwilongo (2025) como fundamentais para a validade da técnica.

As sessões foram moderadas pelo autor da dissertação Omar Soares, com o apoio e participação do orientador da dissertação (Professor Doutor José Agostinho de Sousa Pinto), de forma a assegurar a neutralidade, a fluidez discursiva e o cumprimento do guião.

As contribuições recolhidas ao longo das sessões de Focus Group foram sistematicamente registadas e analisadas em tempo real, com base em notas detalhadas e observações diretas. As sugestões, comentários críticos e consensos emergentes foram incorporados de forma progressiva e fundamentada no processo de adaptação do plano de negócios. Este procedimento permitiu alinhar o modelo de negócio do KIS com as perceções e recomendações dos participantes, para assegurar uma validação empírica contínua e uma reformulação orientada pelas evidências obtidas durante as discussões.

4 Focus Group – Modelo de Negócio KIS

A validação empírica de um modelo de negócio é uma etapa crítica no processo de construção de soluções tecnológicas orientadas ao mercado.

No contexto desta investigação, a metodologia de *Focus Group* foi aplicada com o objetivo de recolher contributos qualificados sobre o plano de negócios do KIS, segundo o *Business Model Canvas*.

Este processo permitiu não só obter o parecer de especialistas, mas também realizar uma análise crítica e colaborativa dos pressupostos estratégicos que fundamentam a proposta de valor do projeto. O *Focus Group* foi essencial para analisar e explorar lacunas e identificar melhorias necessárias à estrutura e coerência do modelo.

Neste enquadramento, o *Focus Group* desempenhou uma função essencial. Por um lado, gerou a possibilidade da recolha de contributos substanciais sobre a adequação da proposta de valor, da estrutura de custos, da lógica de receita, dos canais e das estratégias de relacionamento com clientes, por outro, tornou visíveis as incoerências, pontos críticos e oportunidades de melhoria que poderiam comprometer a exequibilidade do plano de negócios. Além de confirmar ou refutar hipóteses, a metodologia foi mobilizada como instrumento de aprendizagem coletiva e de aperfeiçoamento estratégico.

Neste sentido, este capítulo está estruturado em quatro secções que refletem a cronologia e a lógica do processo de validação.

- A primeira secção descreve o estado inicial do plano de negócios antes da realização das sessões.
- A segunda apresenta a estrutura do *Focus Group*, relativamente aos seus critérios de seleção dos participantes, a estrutura das sessões e os procedimentos de registo e análise.
- A terceira sistematiza os resultados obtidos durante as sessões, organizados em torno dos nove elementos do *Business Model Canvas*.
- A quarta secção discute as alterações introduzidas no plano com base nos contributos recolhidos, e evidencia o valor do *Focus Group* como ferramenta de co-criação e de refinamento estratégico.

4.1 Estrutura do Plano de Negócios antes do Focus Group

Antes da realização das sessões de *Focus Group*, o plano de negócios do projeto KIS encontrava-se numa fase estruturada, embora ainda preliminar, que refletia uma proposta de valor clara e ambiciosa, assente em pressupostos estratégicos com um desenvolvimento sustentado no *Business Model Canvas*.

O plano tinha como base a criação de um dispositivo multifuncional centrado em três funcionalidades principais: autenticação biométrica, gestão segura de acessos e *cold storage* (método de armazenamento de dados em dispositivos físicos) de criptoativos, com integração opcional de backups em cloud. Estas funcionalidades visavam responder aos principais desafios atuais de segurança digital, nomeadamente a vulnerabilidade das palavras-passe tradicionais, a complexidade na gestão de acessos e o risco de perda ou roubo das palavras-passe.

No que diz respeito à proposta de valor, o KIS posicionava-se como uma solução de segurança digital inovadora, simples e fiável, diferenciando-se por concentrar, num único dispositivo, funcionalidades críticas habitualmente dispersas em diferentes plataformas e dispositivos.

Pretendia substituir a tradicional autenticação por palavras-passe por autenticação exclusivamente biométrica, eliminar a dependência de múltiplas contas e aplicações, e oferecer uma *cold wallet* integrada para proteção offline de criptoativos, associada a funcionalidades complementares de *backup* em *cloud*. Esta combinação de fatores sustentava a promessa de uma experiência de utilização mais segura, integrada e intuitiva.

O segmento de clientes definido inicialmente dividia-se em dois grandes grupos: o segmento B2C, composto por utilizadores individuais com literacia digital moderada a elevada e/ou investidores em criptoativos e o segmento B2B, dirigido a empresas com elevada rotatividade de recursos humanos, necessidade de onboarding e offboarding seguro, bem como a gestores de fundos ou ativos digitais.

O plano propunha uma abordagem híbrida, capaz de responder a diferentes perfis de utilização, com comunicação e funcionalidades adaptadas a cada contexto.

No elemento dos canais, a estratégia delineada previa três eixos principais de distribuição:

1. Loja de e-commerce própria, com entrega direta ao consumidor ou a pontos de recolha;
2. Presença em lojas de retalho especializadas como FNAC, Worten ou MediaMarkt, visando públicos menos propensos à compra online;
3. Parcerias logísticas com operadores como CTT, FedEx ou DHL, consoante a geografia do consumidor final.

O plano considerava também, numa fase posterior, a presença em marketplaces digitais como Amazon ou eBay, embora esta opção ainda não estivesse plenamente estruturada.

Relativamente ao relacionamento com o cliente, o plano propunha a adoção de sistemas CRM para segmentação de vendas, apoio técnico online e a disponibilização de conteúdos digitais como FAQs ("*Frequently Asked Questions*" ou "Perguntas Frequentes"), um blog de cibersegurança e testemunhos de clientes. Esta estratégia visava construir a confiança com o cliente e transmitir a autoridade da marca no domínio da proteção de dados e da segurança digital, mesmo ao considerar a limitação de recursos típica de uma *startup*.

No elemento de fontes de receita, o modelo previa dois mecanismos principais:

1. A venda do dispositivo, com um preço unitário estimado de 280€.
2. Uma subscrição mensal complementar, centrada na oferta de maior capacidade de backup em cloud.

Esta segunda via de monetização visava assegurar uma receita recorrente e adaptável a diferentes necessidades dos utilizadores. No entanto, tal como se veio a verificar nas sessões do Focus Group, a aceitação de uma funcionalidade de cloud para um dispositivo de segurança foi posteriormente questionada.

Quanto aos recursos-chave, o plano assentava numa equipa multidisciplinar, composta por especialistas em engenharia informática, design de produto, segurança digital, gestão e direito empresarial.

Do ponto de vista tecnológico, os recursos incluíam tecnologias biométricas (leitores de impressão digital), comunicação sem fios (NFC, Bluetooth), chips criptográficos e compatibilidade com diversos sistemas operativos e dispositivos.

As atividades-chave identificadas eram o desenvolvimento tecnológico contínuo (funcionalidades e atualizações de segurança) de modo a garantir a proteção necessária contra ameaças virtuais emergentes, o marketing digital e a comunicação institucional (campanhas, redes sociais, parcerias com influenciadores e participação em eventos de inovação como o Web Summit), e a negociação e manutenção de parcerias comerciais e tecnológicas.

No elemento das parcerias-chave, estavam nomeadas entidades específicas, como a Thales (Gemalto), OKTA, Fingerprint Cards e NXP, como potenciais fornecedores ou parceiros de componentes e tecnologia. A proposta visava criar um ecossistema tecnológico eficaz e credível, ainda que os próprios participantes do Focus Group tenham vindo a sugerir a substituição destas referências por categorias genéricas (ex.: fornecedores de sensores biométricos, integradores de segurança, produtores de semicondutores), devido ao caráter exploratório do projeto.

Por fim, a estrutura de custos previa despesas com desenvolvimento tecnológico, aquisição de componentes, produção, marketing, logística e apoio ao cliente. O custo por unidade de produção estava estimado em 140€, com margens projetadas para permitir retorno sobre o investimento a partir do segundo ano de atividade, ao considerar uma estratégia de crescimento progressiva e assente em parcerias através de valores meramente especulativos.

Apesar da clareza e coerência geral do plano, havia ainda diversos pontos a validar, aprofundar e melhorar, entre os quais: a perceção do valor real do dispositivo por parte dos segmentos identificados, a aceitabilidade da autenticação biométrica como método exclusivo de acesso, a resistência à aquisição de dispositivos de segurança via canais online, a pertinência de um modelo de subscrição e a combinação, num só produto, das funções de carteira de acessos e criptoativos.

Estas questões fundamentaram a necessidade de realizar as sessões de *Focus Group*, com o objetivo de recolher contributos especializados e fundamentar empiricamente os ajustes estratégicos necessários à consolidação do modelo de negócio.

4.2 Estrutura e Realização do Focus Group

A metodologia de *Focus Group* foi selecionada para esta investigação pela sua capacidade de promover um ambiente dinâmico de interação entre especialistas, permitir a validação e recolha de dados qualitativos úteis e em contexto de discussão aberta e estruturada. Esta abordagem é particularmente adequada para explorar perceções, validar hipóteses e identificar aspetos latentes não considerados na formulação inicial de modelos de negócio, como sublinham Lane et al. (2001) e Mwilongo (2025).

No presente estudo, o *Focus Group* teve como principal finalidade a análise e validação crítica dos nove elementos do modelo de negócio do KIS, tal como definidos no *Business Model Canvas*, ao considerar contributos oriundos de perfis académicos e profissionais com experiência multidisciplinar.

A estrutura metodológica seguiu os princípios clássicos da técnica, conforme estabelecidos por Morgan (2021), ao ser adotado um formato de duas sessões síncronas virtuais, organizadas sequencialmente. A realização remota foi adotada por razões de conveniência e disponibilidade dos participantes, sem comprometer os princípios fundamentais da técnica.

A composição do grupo incluiu quatro participantes, todos Professores Doutores da área das ciências empresariais, metodologias e das tecnologias de informação, selecionados por conveniência e relevância académica e profissional para o tema em estudo:

- Professor Doutor José Agostinho (orientador da dissertação)
- Professor Doutor Pedro Mendonça
- Professor Doutor Rui Umberto
- Professor Doutor Luís Rodrigues

A moderação foi assegurada pelo autor da dissertação (Omar Soares), com apoio do orientador Professor Doutor José Agostinho de Sousa Pinto, e baseou-se num guião temático previamente validado na primeira sessão de *Focus Group*, com questões abertas orientadas à análise crítica dos nove elementos do *Business Model Canvas*, assim como à validação da viabilidade prática da proposta de valor do dispositivo KIS.

As sessões foram conduzidas através de videoconferência, recorrendo a plataforma digital ZOOM com funcionalidades de partilha de ecrã e moderação interativa. Foram respeitadas as recomendações de Ning et al. (2024) quanto à importância de fatores situacionais (mesmo em ambiente digital) e assegurado a qualidade da comunicação, a clareza dos materiais apresentados e a equidade de participação entre os participantes.

A primeira sessão, com duração aproximada de 1 hora, teve um caráter exploratório e preparatório e teve como objetivo apresentar detalhadamente o dispositivo KIS, os seus concorrentes diretos, o panorama de mercado e os elementos estruturais do modelo de negócio. A discussão centrou-se, nesta fase, na identificação das áreas de maior relevância e nas componentes estratégicas consideradas prioritárias para discussão.

A segunda sessão, com duração aproximada de 2 horas, centrou-se exclusivamente na discussão aprofundada dos temas identificados na primeira sessão. Foram abordadas, de forma estruturada, as perceções dos participantes quanto à proposta de valor, segmentos de clientes, canais de distribuição, modelo de receita, recursos e parceiros-chave, atividades críticas e a forma de relacionamento com o cliente.

As questões foram formuladas de modo a estimular contributos argumentados e construtivos, promover o cruzamento de perspetivas e a avaliação das diferentes dimensões de viabilidade do modelo e do dispositivo.

Ao longo das sessões, enquanto investigador assumi uma postura de gestão neutra, para assegurar o equilíbrio na participação dos intervenientes e a manutenção do foco temático.

A transcrição das análises, questões e propostas das sessões serviu de base para a análise posterior, ao permitir identificar padrões discursivos, sugestões consensuais e divergências analíticas relevantes. A riqueza e profundidade dos contributos obtidos validaram a adequação metodológica do *Focus Group* como técnica central de validação e recolha de dados nesta dissertação.

A secção seguinte apresenta os principais resultados emergentes das discussões, sistematizados por elementos do *Business Model Canvas*.

4.3 Resultados

A discussão realizada nas sessões de Focus Group foi organizada com base nos nove elementos do *Business Model Canvas*, que respeitou uma ordem sequencial previamente definida e apresentada aos participantes. O contributo dos especialistas permitiu identificar ajustes concretos e fundamentados ao plano de negócios inicialmente delineado.

Segmentos de Clientes

A apresentação inicial do segmento híbrido B2C e B2B suscitou consenso quanto à sua adequação. Os participantes validaram a proposta de abranger tanto utilizadores individuais (utilizadores digitais e/ou detentores de criptoativos) como empresas (particularmente aquelas com elevada rotatividade de colaboradores). Foi sugerido que o design do dispositivo e a comunicação fossem adaptados aos dois segmentos, de forma a existir variações visuais ou funcionais entre as versões orientadas para cada público.

Canais

A apresentação dos canais de distribuição do KIS incluiu três vias principais:

1. Loja de e-commerce própria.
2. Pontos de venda físicos em retalhistas especializados.
3. Parceiros de logística para entrega direta.

Esta estrutura visava maximizar o alcance e a conveniência para o consumidor final e respeitar os diferentes perfis de compra. Contudo, a discussão revelou várias recomendações importantes que levaram a uma reavaliação crítica desta estratégia.

Os participantes manifestaram preocupação com a fiabilidade do canal online, especialmente ao considerar a natureza sensível do produto. Foi sugerida a inclusão de vendas em marketplaces digitais como forma de aumentar a visibilidade e acessibilidade do dispositivo e consequentemente reduzir os custos da gestão de um site e-commerce numa fase inicial, nomeadamente plataformas como Facebook Marketplace e lojas online de grandes retalhistas (ex: Worten, FNAC). Esta abordagem permitiria atingir públicos diversificados e gerar mais confiança através da credibilidade das plataformas intermediárias.

Adicionalmente, foi expressa a reflexão relativa à integridade do produto durante o processo de distribuição. A possibilidade de clonagem ou substituição do dispositivo durante o transporte foi apontada como um risco real. Para mitigar esse risco, os participantes propuseram três medidas concretas:

1. Selagem inviolável e numerada das embalagens.
2. Criação de um sistema de ativação segura, com envio de um código único ao comprador por canais autónomos (e-mail ou SMS).
3. Reforço da rastreabilidade do dispositivo entre a fábrica e o cliente final.

Estas sugestões visam reforçar a confiança no canal digital e proteger a autenticidade do produto.

Por fim, foi proposta uma alteração estratégica, em vez de iniciar com uma loja de e-commerce própria, o projeto deveria lançar primeiro um website institucional com a listagem dos pontos de venda e canais autorizados. Esta opção permitiria adiar o investimento direto na criação e gestão de um site de e-commerce e validar os canais através de parceiros já estabelecidos. A venda presencial continuaria a ser uma via relevante, sobretudo para perfis de consumidores que valorizam o contacto físico com o produto e o processo de compra assistida.

3. Relacionamento com o Cliente

Este elemento foi discutido com o objetivo de avaliar quais as estratégias de interação e de suporte que seriam mais adequadas à segmentação do KIS, de forma a garantir confiança, continuidade da utilização e reforço da proposta de valor.

Inicialmente, foi apresentada a estratégia delineada no plano de negócios, que previa a utilização de ferramentas de CRM (Customer Relationship Management) para monitorizar vendas, perfis de clientes e canais de aquisição. Estava igualmente prevista a disponibilização de apoio técnico online, aliado à criação de conteúdos digitais como FAQs, tutoriais e blogues educativos sobre segurança digital.

Durante a discussão, os participantes sublinharam que o fator central para garantir uma relação eficaz com os clientes do KIS residia na transmissão de confiança e credibilidade do dispositivo e da marca, aspetos particularmente sensíveis num produto centrado na segurança digital e proteção de criptoativos.

Nesse sentido, foi amplamente consensual que a simples disponibilização de apoio técnico tradicional seria insuficiente. Em alternativa, foi sugerido investir numa consultoria técnica especializada, com foco em boas práticas de utilização do dispositivo, gestão de riscos, manutenção do dispositivo e procedimentos a seguir em caso de avaria.

Esta orientação permitiria construir uma relação de maior valor com os clientes, sobretudo os do segmento empresarial (B2B), cujas necessidades são mais complexas e críticas. Acrescentou-se que, uma vez que o KIS é um projeto em fase de lançamento e constituído por uma estrutura ainda limitada (característica típica de uma start-up), o relacionamento com o cliente deve ser seletivo e focado nos serviços essenciais, de modo a manter a viabilidade operacional. Essa orientação pragmática foi valorizada, alertando para o risco de prometer demasiados serviços que poderiam não ser exequíveis com os recursos disponíveis inicialmente.

No seguimento da reflexão estratégica, surgiu ainda a necessidade de definir com clareza o posicionamento do produto, se orientado para um mercado de massas, onde o fator preço é mais sensível, ou para nichos de utilizadores altamente exigentes, dispostos a pagar mais por uma solução de segurança diferenciada. A recomendação partilhada foi optar inicialmente por um posicionamento de nicho, com maior foco na eficácia e segurança do que na acessibilidade económica.

Como proposta de diferenciação e resposta às distintas necessidades identificadas entre os segmentos B2C e B2B, foi sugerida a criação de duas versões do produto:

- KIS Light - Orientado para utilizadores individuais focados apenas na gestão segura de acessos.
- KIS - Mais completo, ao incorporar também funcionalidades de armazenamento e proteção de criptoativos.

Esta segmentação permitiria adaptar o relacionamento com o cliente às particularidades de cada público-alvo, ao promover uma experiência personalizada e ajustada às suas expectativas e exigências. Em síntese, a discussão em torno do relacionamento com o cliente revelou a importância de um serviço pós-venda orientado à educação, confiança e especialização, mais do que ao suporte técnico convencional, e destacou a necessidade de alinhar a estrutura relacional com os recursos disponíveis e o posicionamento estratégico do negócio.

Fontes de Receita

O elemento Fontes de Receita foi abordado com o intuito de discutir as alternativas economicamente viáveis para sustentar o projeto KIS, ao assegurar simultaneamente a competitividade no mercado e retorno financeiro adequado. O plano de negócios inicial propunha duas vias principais de geração de receita:

1. Venda direta do dispositivo KIS.
2. Modelo de subscrição mensal, associado à expansão da capacidade de backup em *cloud*.

Durante o *Focus Group*, esta estrutura de receitas foi objeto de debate crítico. As questões colocadas aos participantes focaram-se na viabilidade de um modelo de subscrição, bem como na disposição do mercado para aceitar um preço mais elevado pelo dispositivo com serviços incluídos ou, alternativamente, um valor base mais acessível com serviços complementares por subscrição.

As respostas apontaram para um posicionamento claro contra a utilização de um recurso cloud para a realização de backups de dados sensíveis, dado o tipo de produto em questão e a sua promessa de segurança total. Os participantes demonstraram alguma apreensão quanto à vulnerabilidade das soluções baseadas em *cloud*, ao sugerir que a funcionalidade de backup online fosse eliminada, privilegiando-se antes mecanismos de backup local ou offline, mais alinhados com o conceito de *cold storage* e com a proposta de valor centrada na autonomia e segurança do utilizador.

Face a estas preocupações, emergiu uma nova proposta: reposicionar o modelo de subscrição não como um serviço de reserva de dados, mas como um plano de suporte evolutivo ao produto, com funcionalidades que acrescentem valor de forma prática e operacional. As sugestões incluíram:

- Troca direta do dispositivo em caso de lançamento de versões mais avançadas, o que permitiria ao cliente manter-se tecnologicamente atualizado.
- Substituição imediata do equipamento em caso de avaria.
- Serviço de consultoria em segurança digital, com recomendações de boas práticas, configurações e orientações personalizadas.
- Acesso prioritário a atualizações críticas e funcionalidades experimentais.

Foi ainda sugerido que, ao invés de aplicar o modelo de subscrição desde o início, se considerasse a sua adoção progressiva, apenas após a validação do produto no mercado. O objetivo seria permitir uma maior flexibilidade de entrada para o consumidor e evitar a percepção de complexidade ou de dependência de serviços adicionais.

Em alternativa ao modelo de subscrição convencional, foi proposto um modelo de financiamento fracionado: o cliente pagaria uma mensalidade reduzida que englobaria o custo do dispositivo e o acesso ao conjunto de serviços mencionados, o que iria criar uma barreira de entrada mais baixa e consequentemente facilitar a adoção inicial, sobretudo no segmento B2C.

Em suma, a funcionalidade de backup em cloud, inicialmente proposta como justificação para a subscrição, foi rejeitada por implicar riscos de segurança e contrariar os princípios de armazenamento local defendidos para dispositivos de segurança. Em contrapartida, foram sugeridos modelos de subscrição baseados em serviços de valor acrescentado como a atualização tecnológica com possibilidade de substituição periódica do dispositivo, assistência premium, e consultoria em cibersegurança. Foi ainda proposto um modelo de aquisição com pagamento fracionado (mensalidade ou anuidade) que incluísse o dispositivo e os serviços, de forma a facilitar o acesso ao produto sem comprometer a sustentabilidade financeira do projeto.

Recursos-Chave e Parcerias-Chave

No âmbito da estruturação do modelo de negócio do KIS, os recursos-chave e os parceiros estratégicos assumem um papel determinante na viabilização e operacionalização da proposta de valor centrada na segurança digital, autenticação biométrica e gestão de criptoativos. Durante a sessão de Focus Group, estes dois elementos foram apresentados em conjunto, dado o seu carácter complementar e interdependente.

Inicialmente, foi salientado que os principais recursos internos identificados no plano de negócios eram de natureza humana e tecnológica. Ao nível dos recursos humanos, foi apontada a constituição de uma equipa multidisciplinar como elemento essencial, composta por perfis especializados nas áreas da gestão empresarial, tecnologias de informação, serviços jurídicos e desenvolvimento e design de produto.

Esta diversidade é considerada fundamental para garantir uma abordagem integrada à conceção, desenvolvimento, conformidade legal e posicionamento de mercado do dispositivo KIS.

Do ponto de vista tecnológico, foram destacados como recursos indispensáveis a incorporação e integração de tecnologias como biometria digital, NFC (“*Near Field Communication*” ou “Comunicação de Campo Próximo”), bluetooth, sensores criptográficos, e compatibilidade multi-plataforma com sistemas operativos e aplicações digitais amplamente utilizadas. Estes elementos constituem a base técnica do produto, sendo também geradores de diferenciação face à concorrência.

No que respeita às parcerias-chave, o plano de negócios inicial propunha o estabelecimento de colaborações com empresas especializadas no fabrico de semicondutores, sensores biométricos, plataformas de gestão de acessos e componentes eletrónicos. Durante a apresentação foram referenciadas empresas específicas do setor, como a Thales Group (Gemalto), a OKTA, a Zhejiang Kingta Electronics e a Fingerprint Cards, que serviram como exemplos ilustrativos da tipologia de parceiros com os quais seria desejável estabelecer relações comerciais.

Contudo, os participantes do Focus Group levantaram uma questão metodológica importante: dado que este projeto se insere no âmbito de uma dissertação de Mestrado, e não de um plano de internacionalização empresarial em curso, a inclusão de nomes específicos de fornecedores e parceiros poderia conferir uma impressão de compromisso ou de maturidade de projeto que ainda não se verifica. Nesse sentido, foi recomendada uma abordagem mais genérica e analítica, com o foco nas áreas tecnológicas e nos mercados estratégicos relevantes (por exemplo, o mercado indiano no setor de desenvolvimento de software e firmware, o mercado nórdico na área de sensores biométricos, e o sudeste asiático na produção de componentes eletrónicos).

Para além das parcerias tecnológicas, os participantes destacaram também a importância de estabelecer alianças em domínios como a promoção, a distribuição e a comercialização, de forma a acelerar a entrada no mercado e reforçar a credibilidade do produto. Foi sugerida, por exemplo, a identificação de canais de distribuição confiáveis, redes de retalho especializadas em tecnologia e parcerias com influenciadores e especialistas na área da cibersegurança, capazes de legitimar a proposta de valor junto de segmentos críticos.

Por fim, a discussão permitiu consolidar a ideia de que os recursos-chave devem ser pensados não apenas como ativos operacionais, mas como condições estruturais para a criação de confiança no mercado. A articulação eficaz entre a equipa, a tecnologia e as parcerias deverá garantir a solidez da execução e o alinhamento entre os objetivos estratégicos e a capacidade real de entrega do produto e dos serviços associados.

Atividades-Chave

As atividades-chave representam os processos críticos e contínuos que garantem a viabilidade operacional e a entrega da proposta de valor do modelo de negócio KIS. No plano inicial, foram identificadas três atividades principais:

1. O desenvolvimento tecnológico.
2. O marketing estratégico.
3. A gestão de parcerias.

Estes vetores foram apresentados no Focus Group como pilares fundamentais para a fase de arranque do projeto e para a construção da sua vantagem competitiva no mercado da segurança digital.

No que respeita ao desenvolvimento tecnológico, foi sublinhada a necessidade de investimento contínuo em investigação e desenvolvimento, com ênfase na criação de novas funcionalidades, melhoria das funcionalidades existentes e, sobretudo, em atualizações regulares de segurança, para garantir a resiliência do dispositivo face a ameaças emergentes. Este ponto foi amplamente reconhecido como essencial, dada a natureza crítica do produto enquanto ferramenta de proteção de acessos e criptoativos. A capacidade de atualização e evolução tecnológica foi apontada como fator-chave para garantir a longevidade e a confiança do cliente.

A segunda vertente abordada foi o marketing digital e relacional, entendido como um motor de visibilidade e de aceitação de mercado. As ações previstas incluem campanhas digitais em redes sociais, produção de conteúdos educativos sobre segurança digital, colaboração com influenciadores e especialistas do setor e participação em eventos de referência na área da tecnologia e inovação (ex: Web Summit). Os participantes reforçaram a importância de que estas ações sejam dirigidas com foco nos públicos-alvo específicos (B2C e B2B), ao ajustar o discurso consoante o nível de literacia digital e as necessidades práticas dos utilizadores.

A terceira linha de atuação apresentada refere-se à gestão ativa de parcerias, tanto tecnológicas como comerciais. Foi reconhecida a relevância da identificação de novos parceiros estratégicos, bem como da manutenção de relações de longo prazo com fornecedores e entidades que acrescentem valor à cadeia de desenvolvimento, produção e distribuição. Esta dimensão será particularmente relevante para escalar o negócio com base em sinergias e credibilidade partilhada.

Durante a sessão de Focus Group, foi colocada a questão “Na sua opinião, estas atividades-chave serão suficientes?”, à qual os participantes responderam unanimemente de forma afirmativa, dado que estas cobrem, de forma adequada, os aspetos fundamentais para a fase primária de lançamento e validação do produto no mercado. Ainda assim, foi implicitamente reconhecida a necessidade de adaptação futura das atividades consoante a evolução do mercado, da empresa e da maturidade tecnológica do produto.

Deste modo, as atividades-chave inicialmente delineadas foram não só validadas, como também reforçadas pela visão crítica dos especialistas presentes na sessão, ao serem consideradas adequadas para garantir a operacionalização da proposta de valor, a sustentabilidade do modelo de negócio e o posicionamento competitivo da solução KIS no mercado da cibersegurança.

Estrutura de Custos

A estrutura de custos não foi debatida com profundidade dado que este projeto se insere no âmbito de uma dissertação de Mestrado e por esse motivo os valores presentes no plano de negócios são meramente especulativos, uma vez que para maior rigor seria necessário um desenvolvimento mais avançado do projeto e orçamentos reais, mas foi reafirmada a importância de uma abordagem concisa para garantir a sustentabilidade durante o processo de validação comercial e industrialização do produto.

Proposta de Valor

A proposta de valor do KIS, foi concebida com o objetivo de responder a um conjunto de necessidades emergentes no domínio da segurança digital pessoal e empresarial. Assente na premissa de que a autenticação biométrica e o armazenamento local e seguro de dados sensíveis representam soluções superiores aos modelos tradicionais baseados em palavras-passe e armazenamento em nuvem, a proposta inicial foi apresentada aos participantes do Focus Group para validação e debate.

Para facilitar a compreensão e promover a identificação com diferentes perfis de utilizadores, foram introduzidas duas personas representativas dos segmentos B2C e B2B. A persona Sofia Marques, utilizadora intensiva de plataformas digitais e detentora de criptoativos, expressa frustração com a necessidade de memorizar múltiplas palavras-passe e receio da perda de acessos. Já o João Ribeiro, Diretor de Sistemas de Informação, lida com responsabilidades críticas de gestão de acessos e proteção de dados em contexto corporativo, e demonstra interesse por soluções seguras, eficazes e de fácil integração em ambientes empresariais complexos. Estas personas ajudaram a contextualizar a proposta de valor do KIS na realidade prática de potenciais utilizadores.

Durante o debate, o KIS foi apresentado como um dispositivo multifuncional que substitui palavras-passe por autenticação biométrica, centraliza a gestão de acessos e criptoativos, oferece controlo personalizado de acessos em ambiente empresarial, armazenamento local de chaves privadas e compatibilidade com múltiplos sistemas.

Os participantes reconheceram o valor da solução proposta, mas apresentaram sugestões críticas e construtivas com implicações diretas na reformulação da proposta de valor.

Um dos primeiros pontos debatidos foi relativo ao tamanho do dispositivo, tendo sido consensual que o mesmo deveria ser compacto e portátil.

As dimensões de 80mm x 40mm x 5mm foram consideradas adequadas, mas reforçou-se a importância de avançar com a construção de um MVP (“Minimum Viable Product” ou “Produto Mínimo Viável”) que possa ser testado com utilizadores finais reais, de forma a recolher feedback contínuo para ajustes de design e funcionalidade.

Sucessivamente, foi sugerida a análise da proposta de valor à luz de três dimensões complementares:

- Atributos intrínsecos: características técnicas, resistência física, design ergonómico e funcionalidades específicas do dispositivo;
- Atributos extrínsecos: embalagem, rótulo, elementos visuais e comunicacionais que influenciam a perceção de qualidade e segurança;
- Atributos intangíveis: reputação da marca, confiança transmitida, experiência de utilização e perceção de segurança.

Um ponto particularmente relevante emergiu da discussão sobre a integração simultânea da carteira de acessos e da carteira de criptoativos no mesmo dispositivo. Foi levantada a preocupação de que, enquanto a gestão de acessos implica a portabilidade constante do dispositivo, os criptoativos são frequentemente armazenados a longo prazo em ambientes físicos seguros, como cofres. A portabilidade do KIS poderia, assim, aumentar o risco de perda ou furto dos ativos. Esta observação conduziu à sugestão de criar dois modelos distintos: um “KIS Light”, focado exclusivamente na gestão de acessos digitais, e um “KIS”, que integraria também a funcionalidade de *cold wallet* para criptoativos, com reforço de mecanismos de proteção.

Ainda neste ponto, os participantes recomendaram o reforço da segurança multifator, não apenas para a ativação inicial do dispositivo, mas também para o seu uso contínuo. A solução proposta incluiu a possibilidade de definir um PIN de desbloqueio para utilização da função de carteira de criptoativos, enviado para o e-mail ou número de telemóvel do utilizador. Este método também serviria como método alternativo em caso de falha da leitura biométrica. Este ajuste responde diretamente à necessidade de garantir segurança sem comprometer a acessibilidade e a experiência de utilização.

Por fim, uma das recomendações mais impactantes foi a eliminação da funcionalidade de backup em cloud, inicialmente prevista no plano de negócios. Os participantes manifestaram preocupações relativamente à exposição de dados sensíveis em ambientes cloud, mesmo que encriptados. A proposta de valor foi, assim, ajustada para se centrar em mecanismos de backup local, alinhando-se com os princípios de segurança descentralizada que caracterizam os utilizadores mais exigentes em matéria de proteção de identidade e ativos digitais.

Em síntese, o Focus Group permitiu validar a orientação estratégica da proposta de valor do KIS, ao mesmo tempo que gerou contributos determinantes para a sua afinação. A combinação entre segurança avançada, simplicidade de uso, compatibilidade com múltiplos sistemas e adaptação às necessidades específicas de diferentes perfis de utilizador revelou-se adequada, desde que acompanhada de opções diferenciadas de produto, mecanismos de proteção reforçados e uma abordagem conservadora à gestão de dados sensíveis. Estes ajustes não só aumentam a atratividade da proposta como consolidam a sua coerência face às expectativas e preocupações do mercado.

4.4 Ajustes e Decisões Estratégicas

A análise crítica resultante das sessões de Focus Group proporcionou um conjunto de contributos relevantes que culminaram em ajustes substanciais e decisões estratégicas fundamentais para a consolidação e amadurecimento do plano de negócios do KIS. A aceitação integral das sugestões dos participantes reflete uma abordagem reiterada e centrada no utilizador, orientada para a maximização da coerência, viabilidade e alinhamento do modelo de negócio com as reais exigências do mercado. Os ajustes incidiram sobre os diversos elementos do Business Model Canvas, onde cada decisão foi sustentada por argumentos empíricos e validações diretas recolhidas nas sessões realizadas.

Segmento de Clientes

Foi validada a orientação para um modelo híbrido B2C e B2B, com segmentações distintas. Esta decisão deriva do reconhecimento, por parte dos participantes, da versatilidade do dispositivo e da sua capacidade de responder simultaneamente às necessidades de segurança digital dos utilizadores individuais e das organizações. Adicionalmente, foi sugerida e aceite a criação de dois modelos distintos do produto: o KIS Light, direcionado para utilizadores domésticos com foco na gestão de acessos, e o KIS, destinado a utilizadores profissionais ou empresariais, ao integrar funcionalidades avançadas como a gestão de criptoativos. Esta bifurcação permite não apenas um posicionamento mais claro por segmento, como também facilita a gestão de preços e estratégias de comunicação diferenciadas. Contudo, esta versão “Light” será apenas desenvolvida após a apresentação do produto KIS ao mercado.

Canais de Distribuição

O plano inicial previa três canais: loja online própria, retalho físico e parcerias logísticas. No entanto, com base no debate, foi decidida a retirada temporária da loja de e-commerce própria (na fase inicial), optando-se por iniciar com um site institucional que apenas indicará os locais autorizados de venda (marketplaces, lojas físicas e distribuidores especializados). Esta decisão visa reduzir os encargos operacionais e reforçar a confiança do consumidor, sobretudo na fase inicial do negócio. Foi também aceite a proposta de incluir marketplaces de elevada visibilidade (como Worten Online e Facebook Marketplace) como canais complementares.

A nível logístico, foi introduzida a ideia de garantir segurança na entrega, através da implementação de um selo inviolável na embalagem e da criação de um mecanismo de ativação multifator (senha única enviada via SMS ou e-mail), de forma a mitigar os receios relacionados com possíveis intervenções maliciosas durante o transporte:



Figura 2 - Embalagem do dispositivo KIS

Nota: Imagem gerada por ChatGPT com os detalhes e requisitos pré-definidos

Relacionamento com o Cliente

As ações inicialmente previstas foram reformuladas para refletir uma abordagem mais realista e centrada em serviços essenciais. Foi decidido que, ao invés de disponibilizar um sistema de apoio técnico extensivo, será implementado um serviço de consultoria técnica e de segurança digital, orientado para boas práticas de utilização e mitigação de riscos.

Paralelamente, foi reforçada a aposta em conteúdos educativos e de sensibilização para a cibersegurança (FAQs, blog, e vídeos explicativos), entendidos como ferramentas fundamentais para reforçar a confiança do utilizador.

A decisão estratégica de iniciar com um foco em segmentos de nicho em vez de massas, mais exigentes e dispostos a pagar por soluções *premium*, implica uma comunicação mais especializada, com menor dispersão de recursos.

Fontes de Receita

Face às preocupações manifestadas relativamente à privacidade e segurança associadas a serviços em *cloud*, foi decidido eliminar a funcionalidade de backup em nuvem do dispositivo KIS. Em alternativa, optou-se por centrar a proposta de valor em soluções de backup local, controladas diretamente pelo utilizador.

Paralelamente, foi redesenhado o modelo de subscrição: ao invés de uma subscrição meramente funcional (ex. armazenamento em cloud), será criada uma subscrição com valor agregado, que inclui:

- Troca direta do dispositivo em caso de lançamento de versões mais avançadas (quando aplicável).
- Substituição imediata do equipamento em caso de avaria.
- Serviço de consultoria em segurança digital, com recomendações de boas práticas, configurações e orientações personalizadas.
- Acesso prioritário a atualizações críticas e funcionalidades experimentais.

Recursos e Parcerias-Chave

Foi aceite a recomendação de não identificar empresas específicas nesta fase académica do projeto e optar por caracterizar os perfis dos parceiros necessários (ex. fornecedores de semicondutores, biometria, restantes componentes) e as localizações geográficas mais promissoras, como Índia e Sudeste Asiático para componentes tecnológicos. Foi ainda introduzida a necessidade de explorar parcerias comerciais e promocionais para ampliar o alcance de mercado, nomeadamente com retalhistas especializados e influenciadores digitais na área de cibersegurança.

Atividades-Chave

As atividades inicialmente previstas foram validadas pelos participantes e foram consideradas adequadas à fase de entrada no mercado. Confirmou-se a importância do desenvolvimento tecnológico contínuo, do marketing digital especializado, da participação em eventos setoriais relevantes (como o Web Summit) e da gestão proativa das parcerias estratégicas.

Estas atividades foram mantidas no plano com ênfase no seu alinhamento com a fase inicial do projeto, priorizando ações com elevado retorno e de validação de mercado.

Estrutura de Custos

A estrutura de custos não foi debatida com profundidade, dado que foi reconhecido que, por se tratar de uma dissertação de Mestrado, os valores presentes no plano de negócios mesmo que estimativos, seriam adequados. Contudo, reafirmou-se a importância de adotar uma abordagem concisa e seletiva na alocação de recursos, com foco nas áreas críticas para a viabilização do projeto e respetiva validação do mercado. A flexibilidade orçamental foi entendida como condição essencial para garantir a sustentabilidade do modelo durante a fase de desenvolvimento, validação e eventual industrialização do produto.

Proposta de Valor

A proposta de valor foi reformulada em função de duas preocupações centrais, o equilíbrio entre portabilidade e segurança, e a clareza na diferenciação de funcionalidades. Foi acolhida a sugestão de rever a integração simultânea da carteira de acessos e de criptoativos no mesmo dispositivo, ao reconhecer que estas funcionalidades implicam padrões distintos de uso e de risco. Assim, reforçou-se a estratégia de segmentação através da criação das versões KIS Light e KIS. Além disso, foram incorporadas sugestões relativas ao design, à embalagem e à marca, de modo a fortalecer a componente intangível da proposta de valor. Adicionalmente, foi aceite a recomendação de integrar uma segurança multifator para a ativação e uso do dispositivo, o que completa a segurança de biometria com alternativas como PIN temporário a ser enviado por um canal seguro.

CAPÍTULO V – CONCLUSÕES E PERSPETIVAS DE DESENVOLVIMENTO

O presente capítulo tem como finalidade concluir a dissertação, ao oferecer uma perspetiva integrada dos principais resultados, implicações e contributos da investigação realizada. Após a contextualização teórica e a revisão de literatura, procedeu-se à formulação de um modelo de negócios sustentável para o dispositivo KIS, cuja proposta de valor assenta na substituição das palavras-passe por autenticação biométrica, aliada à gestão segura de acessos e ao armazenamento local de criptoativos.

O plano de negócios concebido foi estruturado com base no modelo Business Model Canvas, como referência metodológica adotada para decompor, analisar e organizar os elementos essenciais à criação, entrega e obtenção de valor. A sua aplicação permitiu explorar, de forma sistemática, os nove elementos que compõem um modelo de negócios completo: proposta de valor, segmentos de clientes, canais, relacionamento com os clientes, fontes de receita, recursos-chave, atividades-chave, parcerias estratégicas e estrutura de custos. Adicionalmente, a estrutura detalhada do plano de negócios, apresentada no Apêndice I, foi elaborada de acordo com o guia explicativo (Anexo 1) "Como Elaborar um Plano de Negócios", disponibilizado pelo IAPMEI – Agência para a Competitividade e Inovação, I.P.. Esta entidade, anteriormente designada como Instituto de Apoio às Pequenas e Médias Empresas e ao Investimento e Instituto de Apoio às Pequenas e Médias Empresas e à Inovação, é um organismo público de referência em Portugal no apoio ao contexto empresarial, sobretudo no que respeita à estruturação estratégica de novos negócios e projetos empreendedores.

Paralelamente, foi adotada uma abordagem qualitativa baseada na metodologia de Focus Group, conduzida em duas sessões online, com participantes convidados pela sua experiência académica e conhecimento especializado em áreas relevantes, tais como segurança digital, inovação tecnológica, sistemas de informação e gestão empresarial. Esta estratégia permitiu recolher perceções, críticas e sugestões dirigidas aos elementos centrais do modelo de negócio, o que constituiu um processo participativo de validação empírica e refinamento do plano proposto.

Com base nesse percurso metodológico, o presente capítulo introduz e estrutura os próximos pontos finais da dissertação, nomeadamente: uma síntese dos principais resultados e conclusões, a identificação de dificuldades e limitações sentidas durante o desenvolvimento do trabalho, e a apresentação de sugestões para desenvolvimentos futuros.

5 Contributos da Investigação

A presente dissertação teve como objetivo responder à questão de investigação “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?”, através da estruturação e validação de um modelo de negócio sustentável, viável e estrategicamente alinhado com as necessidades do mercado da segurança digital. A proposta de valor desenvolvida materializa-se no KIS – Keep It Safe, um dispositivo multifuncional que conjuga, num único artefacto físico, mecanismos de autenticação biométrica, gestão integrada de acessos, e uma solução segura de armazenamento local para criptoativos.

A investigação foi iniciada com uma análise aprofundada do contexto tecnológico e das fragilidades dos modelos tradicionais de autenticação, particularmente o uso de palavras-passe. A revisão de literatura revelou que, apesar das recomendações sobre complexidade e diversidade de senhas, os utilizadores persistem em práticas inseguras, motivadas por limitações cognitivas, falta de literacia digital e perceção limitada de risco.

Esta constatação fundamentou a adoção da biometria como alternativa principal, não apenas por eliminar a necessidade de memorização, mas também por permitir um modelo de autenticação mais resistente a diversas tipologias de ataques. Contudo, a literatura e os resultados da metodologia *Focus Group* também advertiram para os riscos associados à irreversibilidade dos dados biométricos, o que justificou a decisão estratégica de garantir que estes dados seriam exclusivamente armazenados de forma local e nunca partilhados com servidores externos ou em ambientes de nuvem.

No que respeita à custódia de criptoativos, foi identificado que o modelo mais seguro continua a ser o armazenamento em *cold wallets*, dada a possibilidade de desconexão da internet e conseqüente redução da superfície de ataque. A integração desta funcionalidade no KIS surgiu, assim, como uma solução coerente e alinhada com as melhores práticas, ao permitir o armazenamento local das chaves privadas, ao evitar a dependência de terceiros ou a exposição a redes comprometidas. Este posicionamento confere ao dispositivo um nível de valor particularmente relevante num ecossistema digital onde a perda ou o comprometimento de ativos digitais é, frequentemente, irreversível.

A estruturação do plano de negócios foi orientada pelo *Business Model Canvas*, que serviu de base para decompor e desenvolver, de forma integrada, os elementos essenciais à criação, entrega e captura de valor. A proposta de valor do KIS, centrada na segurança, simplicidade e integração, foi articulada com segmentos de clientes distintos (B2C e B2B), canais de distribuição viáveis, atividades e recursos-chave, parcerias tecnológicas estratégicas, fontes de receita e estrutura de custos. Esta primeira versão do plano foi posteriormente submetida a validação por meio da metodologia qualitativa de *Focus Group*.

A realização do Focus Group, com especialistas académicos em sistemas de informação, gestão, informática e metodologias de investigação, permitiu analisar criticamente cada um dos nove elementos do modelo de negócio e recolher contributos valiosos para a sua afinação. Os participantes reconheceram o potencial do KIS como uma proposta inovadora, com forte valor diferencial face às soluções existentes, nomeadamente por integrar, de forma coesa e acessível, funcionalidades habitualmente dispersas e tecnicamente complexas. Foi confirmada a adequação do duplo posicionamento nos segmentos B2C e B2B, embora tenha sido recomendada a diferenciação visual ou funcional entre versões destinadas a utilizadores individuais e profissionais, como forma de reforçar a adequação da solução às expectativas de cada público.

No que respeita aos canais de distribuição, as perspetivas recolhidas revelaram preocupações legítimas quanto à fiabilidade do canal de venda online, tendo sido sugerida a utilização de marketplaces reconhecidos e parcerias com retalhistas especializados como forma de gerar confiança e facilitar o acesso ao dispositivo. Adicionalmente, foram levantadas questões sobre a integridade física do produto durante o transporte, recomendando-se a implementação de mecanismos de selagem inviolável e ativação autenticada, de modo a mitigar riscos de substituição ou violação durante a cadeia logística.

A proposta de subscrição de serviços complementares foi objeto de análise crítica, com reservas expressas relativamente à introdução de funcionalidades em nuvem numa solução cujo principal valor reside precisamente na segurança local e na extinção de pontos de falha externos. Estas observações resultaram numa reconfiguração do modelo de obtenção de receitas e numa clarificação da proposta de valor.

A metodologia do *Focus Group* demonstrou elevada adequação à fase exploratória da investigação, ao permitir o cruzamento de perspetivas técnicas e estratégicas e a identificação de dimensões menos visíveis no plano inicial, como a importância da confiança na marca, a sensibilidade do canal de venda e a perceção de risco associada à autenticidade do dispositivo. Esta validação empírica reforçou a coerência interna do modelo de negócios e permitiu a sua afinação em aspetos centrais para a sua operacionalização futura.

Desta forma, para responder à questão “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?” foi possível concluir que o principal valor da técnica reside na sua capacidade de revelar fragilidades estratégicas e perceções subjetivas dos utilizadores que não seriam evidenciadas apenas por métodos quantitativos ou análise documental.

A resposta à questão de investigação não se encontra apenas na capacidade de conceber um artefacto funcional, mas sobretudo na articulação estratégica entre a proposta de valor, o segmento de mercado, os canais de distribuição, o relacionamento com o cliente, os recursos necessários e os mecanismos de monetização que assegurem a sustentabilidade da iniciativa. A metodologia permitiu validar essa articulação à luz de expectativas e exigências reais do mercado.

O KIS poderá representar uma solução com elevado potencial de inserção no mercado, precisamente por responder a uma necessidade real, com um posicionamento claro e uma estrutura estratégica que integra tecnologia, segurança, experiência do utilizador e viabilidade operacional, mas sem a devida sustentabilidade dos elementos validados na metodologia Focus Group, rapidamente se tornará inviável.

Esta dissertação contribui, assim, para o conhecimento da interseção entre segurança online, inovação tecnológica e modelos de negócio, ao demonstrar que a introdução de soluções integradas exige uma abordagem sistémica e centrada no utilizador.

O KIS emerge, portanto, como uma resposta coerente, inovadora e orientada para o mercado, num cenário em que a segurança digital é simultaneamente um imperativo técnico, social e estratégico.

5.1 Síntese dos Resultados

A presente investigação partiu da identificação de um desafio real no domínio da segurança digital: a fragmentação das soluções existentes para autenticação, gestão de acessos e proteção de criptoativos. Em resposta, foi proposto o desenvolvimento de um dispositivo físico multifuncional (o KIS) concebido para integrar, num único artefacto, autenticação biométrica, gestão segura de acessos e armazenamento offline de criptoativos. A dissertação e investigação não se centrou no desenvolvimento técnico do produto, mas antes na estruturação, validação do modelo de negócio e respetiva proposta de valor que viabiliza a sua implementação no mercado, através de uma abordagem sustentada em evidências teóricas.

Com base numa revisão de literatura focada em cinco áreas fundamentais (modelos de negócio digitais, autenticação biométrica, gestão de palavras-passe, proteção de criptoativos e segurança e privacidade de dados) foi possível enquadrar o KIS como uma resposta inovadora e necessária num ecossistema digital cada vez mais vulnerável e exigente. Esta fundamentação teórica confirmou que a dependência de palavras-passe permanece um dos maiores riscos de segurança, que os utilizadores revelam baixa literacia digital e que a biometria, aliada ao armazenamento local e encriptado, representa uma alternativa segura e cada vez mais aceite.

A estruturação do modelo de negócio foi realizada com recurso ao Business Model Canvas, o qual permitiu decompor a proposta em nove elementos estratégicos. Esta estrutura serviu de base para a sessão de *Focus Group*, na qual participaram quatro especialistas académicos das áreas de gestão, sistemas de informação, informática e metodologias de investigação. As sessões permitiram validar a proposta de valor, identificar pontos críticos e recolher recomendações estratégicas que consequentemente reforçaram a coerência, viabilidade e exequibilidade do plano de negócios.

Entre os contributos mais relevantes do *Focus Group* destacam-se a validação do duplo posicionamento nos segmentos B2B e B2C, a importância da diferenciação entre versões para públicos distintos, a necessidade de garantir canais de distribuição que transmitam confiança, e a rejeição de funcionalidades críticas dependentes da cloud. As recomendações permitiram ajustar o modelo de obtenção de receita, reforçar a proposta de valor centrada na autonomia e segurança local, e aperfeiçoar os elementos operacionais e comunicacionais fundamentais para o sucesso comercial do produto.

Neste contexto, a resposta à questão de investigação “Como Conceber um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe?” torna-se clara, o Focus Group revelou-se um instrumento metodológico eficaz para detetar as fragilidades e oportunidades estratégicas do modelo de negócio numa fase inicial. A técnica permitiu validar a proposta a partir de perspetivas práticas e fundamentadas, ao expor as preocupações e critérios de decisão que dificilmente seriam captados por métodos exclusivamente teóricos ou quantitativos.

O contributo específico do Focus Group refletiu-se na identificação de aspetos críticos como a perceção de segurança nos canais de distribuição, a coerência entre proposta de valor e funcionalidades, a sensibilidade ao modelo de monetização e a importância da confiança na marca. Estes elementos, embora pouco desenvolvidos na formulação inicial, revelaram-se essenciais para a maturação da proposta e reforço da sua viabilidade de mercado.

Em suma, esta dissertação demonstrou que é crucial estruturar um modelo de negócio eficaz e sustentável para um dispositivo de segurança digital com uma forte componente tecnológica, desde que esse modelo seja construído com base em pressupostos validados, centrado nas necessidades e perceções dos utilizadores e sustentado por uma proposta de valor clara, distinta e credível. O KIS surge, assim, como uma solução alinhada com os desafios atuais da cibersegurança, e como um exemplo de como a integração entre tecnologia, estratégia e foco no utilizador pode gerar inovação com um possível impacto no mercado.

5.2 Dificuldades e Limitações do Trabalho

Apesar da consistência metodológica e da articulação entre fundamentação teórica, análise e desenvolvimento estratégico, a presente investigação enfrentou um conjunto de dificuldades e limitações que importa reconhecer, tanto pela sua relevância intrínseca como pela utilidade que representam para trabalhos futuros.

A escolha da metodologia qualitativa, ainda que adequada à fase exploratória e ao objetivo de aprofundar perceções, acarreta também as suas limitações inerentes.

Os resultados obtidos são, por natureza, interpretativos e situacionais, e não permitem inferências estatísticas ou generalizações universais.

A validade externa dos dados depende, portanto, da sua triangulação com outras fontes e metodologias, nomeadamente abordagens quantitativas ou testes experimentais com utilizadores reais, em contextos de uso concreto do dispositivo.

Contudo essa limitação foi principalmente originada dada a natureza conceptual do dispositivo KIS e da fase em que este se encontrava no momento da investigação. O facto de não existir ainda um protótipo físico funcional dificultou a recolha de perceções mais práticas por parte dos participantes no Focus Group, que tiveram de basear os seus contributos em descrições técnicas, simulações visuais e explicações teóricas. Embora o guião de discussão tenha sido cuidadosamente estruturado para facilitar a compreensão e promover a reflexão crítica, a ausência de um dispositivo tangível impediu a avaliação direta da experiência de utilização, do design físico e da interação real com o dispositivo. Esta limitação condicionou algumas análises, nomeadamente no que respeita à sua utilização, à ergonomia e à perceção de qualidade do produto.

Devido à fase de desenvolvimento do produto, do ponto de vista do modelo de negócio, uma dificuldade adicional prendeu-se com a avaliação da disposição dos consumidores para pagar por soluções de segurança digital pessoal, sobretudo num mercado ainda pouco maduro e com perceções ambivalentes quanto ao valor da segurança proativa.

A análise de preços, canais e estratégias de monetização teve de basear-se em suposições e análise de soluções já existentes (concorrentes diretos) com soluções parcialmente comparáveis, o que introduz um nível de incerteza inevitável. Ainda que o plano de negócios tenha sido estruturado de forma rigorosa e informado por boas práticas, a sua aplicabilidade concreta dependerá de variáveis contextuais e da evolução dinâmica do mercado, que não podem ser totalmente antecipadas em sede de dissertação académica.

Em conclusão, apesar das limitações aqui identificadas não comprometerem a validade do trabalho realizado, alertam para a complexidade envolvida na transição entre uma proposta conceptual e a sua materialização prática e comercial. Reconhecer estas restrições constitui um exercício essencial de rigor académico e uma base sólida para o desenvolvimento do projeto em fases subsequentes.

5.3 Trabalhos Futuros

Ao considerar o carácter exploratório da presente dissertação e o facto de se encontrar numa fase predominantemente conceptual e estratégica do projeto KIS – Keep It Safe, são identificadas diversas linhas de continuidade que irão permitir desenvolver, materializar e valorizar a investigação realizada, quer em contexto académico, quer em contexto de inovação tecnológica aplicada. Os resultados obtidos, particularmente a validação qualitativa do modelo de negócio proposto e a identificação de necessidades reais de mercado, reforçam a oportunidade e a relevância de investir em novas etapas que transformem o projeto de uma proposta estruturada para uma realidade funcional e potencialmente comercializável.

A primeira etapa do trabalho futuro consiste na elaboração de um artigo científico com o título “Conceção de um Modelo de Negócio no Setor da Segurança Digital: O caso KIS – Keep It Safe”.

Este artigo terá como objetivo sintetizar os principais contributos da dissertação numa estrutura adequada à publicação em revistas científicas ou conferências da área dos sistemas de informação, negócio eletrónico ou inovação tecnológica, ao permitir partilhar os resultados com a comunidade académica e receber críticas construtivas que possam informar fases posteriores do projeto.

A segunda etapa de trabalho prende-se com a necessidade de aprofundar a análise técnica e tecnológica do dispositivo KIS, algo que, por razões de delimitação e foco metodológico, não foi abrangido nesta dissertação. Esta fase implicará o levantamento e avaliação das opções viáveis no que respeita à arquitetura de hardware (processadores seguros, sensores biométricos, chips de encriptação, módulos de armazenamento físico inviolável), ao desenvolvimento de firmware específico, à implementação de políticas de isolamento funcional e à análise de compatibilidade com dispositivos e sistemas operativos existentes.

Esta análise técnica irá incluir igualmente o estudo de normas e certificações de segurança aplicáveis, tanto para o segmento B2C como B2B, de forma a assegurar que o desenvolvimento do produto se alinhe com os padrões de integridade necessários, confidencialidade e disponibilidade.

A ausência deste trabalho técnico detalhado representa uma limitação reconhecida da presente investigação e, simultaneamente, uma oportunidade para continuidade do projeto em contexto de investigação aplicada ou desenvolvimento experimental.

Uma terceira etapa de continuidade passa inevitavelmente pelo desenvolvimento de um protótipo funcional do KIS. Este protótipo permitirá a concretização física dos princípios que sustentam a proposta de valor do dispositivo, e será essencial para a realização de testes reais de utilização, resistência, fiabilidade e segurança.

O protótipo servirá igualmente como base para ensaios exploratórios com utilizadores finais, para permitir a recolha de dados empíricos sobre a experiência de utilização, a curva de aprendizagem, a aceitação das funcionalidades integradas e a confiança transmitida pelo produto. Esta validação prática será crucial para aferir a correspondência entre o modelo de negócio e a realidade operacional, para ajustar funcionalidades ou decisões de design antes da entrada de uma eventual fase de industrialização ou pré-comercialização.

Por último, encontra-se prevista a submissão de uma candidatura ao programa Born From Knowledge (BFK), promovido pela Agência Nacional de Inovação, S.A. (ANI), em representação do Instituto Superior de Contabilidade e Administração do Porto (ISCAP).

Esta candidatura será suportada pelo plano de negócios desenvolvido ao longo da presente dissertação e tem como objetivo obter financiamento, apoio técnico e visibilidade institucional para dar continuidade ao projeto KIS numa lógica de valorização do conhecimento gerado em contexto académico. A participação no programa BFK representaria um passo estratégico na transição do projeto para uma fase de desenvolvimento tecnológico, ao permitir consolidar parcerias, testar hipóteses em contexto de incubação e integrar redes de inovação nacional. A ANI, enquanto entidade promotora da investigação aplicada e da transferência de tecnologia, constitui um parceiro natural para iniciativas desta natureza, que assentam na conversão de conhecimento académico em soluções com aplicabilidade social e económica.

Estas quatro linhas de ação, interdependentes e complementares, irão configurar um plano de desenvolvimento coerente que visa assegurar a continuidade do projeto KIS, ao promover a sua maturação conceptual, materialização técnica, validação prática e reconhecimento institucional.

REFERÊNCIAS BIBLIOGRÁFICAS

- Altarawneh, M. H. M., Althunibat, A., Almajali, M. H., Alzriqat, N., & Alazzam, S. (2025). Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps. *International Journal of Innovative Research and Scientific Studies*, 8(1), 1516–1529. <https://doi.org/10.53894/ijirss.v8i1.4696>
- Balamurugan, M. (2024). Biometric Authentication: A Double-Edged Sword for Security? *International Journal of Science and Research (IJSR)*, 13(9), 170–173. <https://doi.org/10.21275/SR24901230354>
- Becker, M., & Bröcker, J.-O. (2021). Business Model Canvas—Overview of the main advantages and disadvantages.
- Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and Opportunities in Password Management: A Review of Current Solutions. *Sri Lanka Journal of Social Sciences and Humanities*, 3(2), 9–20. <https://doi.org/10.4038/sljssh.v3i2.96>
- Gajjar, N. T. (2024). Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies. 5(4).
- Kaiser, A. F. (2016). Privacy and security perceptions between different age groups while searching online.
- Kirobo, A. R. (2025). Security Vulnerabilities of Cryptocurrency Wallets -A Systematic Review. *FUOYE Journal of Engineering and Technology*, 9(4), 580–590. <https://doi.org/10.4314/fuoyejet.v9i4.4>
- Lane, P., McKenna, H., Ryan, A. A., & Fleming, P. (2001). Focus group methodology. *Nurse Researcher*, 8(3), 45–59. <https://doi.org/10.7748/nr2001.04.8.3.45.c6157>
- Master, A. (2022). Password Managers: Secure Passwords the Easy Way. Purdue University. <https://doi.org/10.5703/1288284317618>
- Morgan, D. L. (2021). Robert Merton and the History of Focus Groups: Standing on the Shoulders of a Giant? *The American Sociologist*, 53(3), 364–373. <https://doi.org/10.1007/s12108-021-09500-5>
- Murray, A., & Scuotto, V. (2015). The Business Model Canvas. *Symphonya. Emerging Issues in Management*, 94–109. <https://doi.org/10.4468/2015.3.13murray.scuotto>

- Mwilongo, N. (2025). Focus Group Discussions in Qualitative Research: Dos and Don'ts. *Eminent Journal of Social Sciences*, 1(1), 1–16. <https://doi.org/10.70582/7fmpzs58>
- Ning, X., Liu, Y., Miao, J. L., & Li, W. L. (2024). Enhancing the Potentials of the Focus Group Discussion – Engaging Frequently Neglected but Essential Situational Factors for Analyzing Data. *International Journal of Qualitative Methods*, 23, 16094069241306332. <https://doi.org/10.1177/16094069241306332>
- Nowroozi, E., Seyedshoari, S., Mekdad, Y., Savaş, E., & Conti, M. (2023). Cryptocurrency Wallets: Assessment and Security. Em Y. Maleh, M. Alazab, & I. Romdhani (Eds.), *Blockchain for Cybersecurity in Cyber-Physical Systems* (Vol. 102, pp. 1–19). Springer International Publishing. https://doi.org/10.1007/978-3-031-25506-9_1
- Santos, J. F., & Pinto, G. (2025). PRIVACIDADE E SEGURANÇA EM SISTEMAS DE INFORMAÇÃO: Uma análise dos aspectos psicológicos e cognitivos envolvidos na percepção e na adoção de medidas de segurança. *Revista Interface Tecnológica*, 21(1), 288–299. <https://doi.org/10.31510/infa.v21i1.1979>
- Sheikh, S. (2024). Biometric Authentication: Enhancing Security and Usability in the Digital Age.
- Haryadi, G. A., Rahaman, M. F., Subhan, M. R., Lee, J. M., & Kim, D. S. (2023). Comparative study of cryptocurrency wallet security: A hybrid, hot, and cold wallet approach. Conference Paper. <https://www.researchgate.net/publication/375187201>
- Tanni, T., Taharat, T., Parvez, M., Rume, S., & Zaber, M. (2022). Is My Password Strong Enough?: A Study on User Perception in The Developing World. *EAI Endorsed Transactions on Creative Technologies*, 9(30), 173452. <https://doi.org/10.4108/eai.11-2-2022.173452>

Apêndice I – Plano de Negócios

SUMÁRIO EXECUTIVO

O presente plano de negócios tem como principal objetivo validar a viabilidade do projeto KIS – *Keep It Safe*, definir as estratégias de implementação, desenvolvimento e crescimento, bem como atrair potenciais investidores, estabelecer parcerias estratégicas e analisar a viabilidade econômica e financeira do projeto.

Nos últimos anos, a cibersegurança emergiu como um fator crítico tanto para indivíduos quanto para empresas, impulsionada pelo aumento significativo de ataques virtuais. Relatórios globais de segurança, como os apresentados pela Cybersecurity Ventures e pela Verizon Data Breach Investigations Report (2024), revelam que milhões de credenciais são comprometidas anualmente, o que resulta em perdas financeiras substanciais e no comprometimento de dados sensíveis, afetando diretamente a confiança dos utilizadores e a integridade das organizações.

Neste contexto, surge a necessidade de um dispositivo eficaz e seguro que ofereça proteção integrada aos utilizadores. O KIS (*Keep It Safe*) é um dispositivo multifuncional que combina autenticação biométrica, gestão segura de acessos e armazenamento de criptoativos. Este produto diferencia-se ao adotar práticas avançadas de segurança e privacidade, ao proporcionar um ambiente digital confiável e acessível. O KIS atende à crescente procura por soluções que eliminam a vulnerabilidade dos acessos tradicionais, como palavras-passe e criptoativos armazenados em sistemas suscetíveis a ataques. Além disso, destaca-se pela sua interface intuitiva, que possibilita o acesso seguro a plataformas digitais sem comprometer a experiência do utilizador.

O público-alvo do KIS divide-se em dois segmentos principais: B2B (“Business to Business” ou “Empresa para Empresa”) e B2C (“Business to Consumer” ou “Empresa para Consumidor”). No segmento B2C, destina-se a utilizadores individuais conscientes e/ou inconscientes da importância da segurança online, que pretendem proteger as suas identidades, dados e ativos digitais sem a necessidade de memorizar múltiplas palavras-passe. No segmento B2B, destina-se a profissionais da área financeira, como gestores de fundos de criptoativos que requerem elevados padrões de segurança para as transações e armazenamento de ativos digitais, e a empresas que precisam de proteger um volumoso conjunto de dados de acesso sensíveis e criptoativos, ao integrar soluções de segurança nas suas infraestruturas existentes.

O KIS facilita a integração de novos funcionários ao eliminar a necessidade de criação constante de acessos, ao permitir a associação de perfis a dados biométricos.

A estratégia de expansão inicial prevê a entrada no mercado europeu, com Portugal como país piloto, seguida pela expansão para regiões altamente digitalizadas e com uma crescente procura por tecnologias de autenticação biométrica e proteção de criptoativos (ex: Japão e Estados Unidos).

A segmentação definida é híbrida, contemplando tanto o mercado B2B (dirigido a empresas com elevada rotatividade de recursos humanos e entidades que gerem ativos digitais críticos) como o mercado B2C (orientado para utilizadores individuais preocupados com a segurança dos seus acessos e criptoativos). No que respeita aos canais de comercialização, será adotada uma estratégia de presença multicanal, com ênfase inicial em pontos de venda físicos e plataformas de marketplaces, na qual a criação de uma loja própria de e-commerce será adiada para fases posteriores do projeto. Esta abordagem permitirá aumentar a acessibilidade do produto e mitigar as preocupações relacionadas com a confiança na entrega.

HISTÓRICO DA IDEIA E/OU DOS PROMOTORES

Motivação Inicial

A conceção do KIS – *Keep It Safe* surge como uma resposta a uma problemática crescente no domínio da segurança online, amplificada pela evolução contínua das tecnologias digitais e a consequente proliferação de ataques informáticos que comprometem a privacidade e a integridade dos dados dos utilizadores.

No contexto do modelo B2C, a motivação principal do projeto é desenvolver ferramentas que enfrentem diretamente as ameaças digitais, ao proporcionar soluções de autenticação eficazes e simplificadas. Estas soluções visam atender a uma crescente necessidade dos consumidores por métodos de autenticação seguros, que não dependam de múltiplas palavras-passe, que são frequentemente vulneráveis a ataques de força bruta ou roubo de credenciais.

Em paralelo, no modelo B2B, o KIS é concebido como uma solução para otimizar a gestão de acessos dentro das organizações, um processo que, tradicionalmente, implica uma carga administrativa elevada.

Em empresas com grande rotatividade de colaboradores ou mudanças frequentes de funções, a criação de acessos e a atribuição de permissões torna-se um processo repetitivo e propenso a erros. O KIS visa resolver essa ineficiência ao permitir que a gestão de acessos seja realizada de forma mais direta e segura, ao associar a impressão digital do colaborador aos seus respetivos "roles" ou permissões já predefinidos no dispositivo, sem a necessidade de criação manual de novos acessos.

Desenvolvimento da Ideia

O desenvolvimento do KIS iniciou-se com um processo de análise abrangente das necessidades do mercado, tanto no contexto B2C como B2B. Foi realizada uma análise detalhada dos principais desafios relacionados com a segurança digital e a gestão de identidades, ao identificar as lacunas nas soluções existentes e as limitações em termos de combinação, eficácia e simplicidade no uso de sistemas de autenticação. A partir desta análise, foram definidas as funcionalidades fundamentais do dispositivo KIS, com o objetivo de responder às necessidades dos utilizadores individuais, em termos de proteção e facilidade de uso, e das organizações, no que respeita à gestão de acessos de colaboradores e à otimização de processos internos.

Identificação do Problema

A principal problemática que o KIS visa resolver é a crescente vulnerabilidade das identidades digitais face a ataques informáticos, tanto no âmbito pessoal (B2C) quanto organizacional (B2B). No âmbito individual, a gestão de múltiplas palavras-passe, frequentemente fracas ou reutilizadas, coloca os utilizadores em risco elevado de ataques informáticos ou de invasões dos seus sistemas digitais pessoais. No contexto organizacional, a criação e gestão de acessos dentro de grandes estruturas corporativas apresenta-se como um desafio, dado que as empresas enfrentam dificuldades em manter o controlo sobre os acessos de colaboradores, especialmente em momentos de integração de novos funcionários ou mudanças de funções. Nesse sentido, o KIS propõe uma solução inovadora que combina autenticação biométrica com a gestão simplificada de permissões de acesso, ao oferecer uma abordagem integrada e segura para resolver estes problemas de forma eficaz.

Soluções Tentadas Anteriormente

As soluções atualmente disponíveis no mercado tendem a concentrar-se em aspetos isolados da segurança digital, como a autenticação MFA ("Multi-Factor Authentication" ou "Autenticação Multi Fator") ou o armazenamento de palavras-passe de forma segura. No entanto, estas abordagens não conseguem, de forma eficaz, integrar múltiplos níveis de segurança num único dispositivo, nem resolver a complexidade da gestão de acessos de forma eficiente. A proposta do KIS distingue-se pela sua capacidade de integrar várias funções de segurança num único dispositivo, como a autenticação biométrica e a gestão de acessos, ao simplificar a experiência do utilizador e, simultaneamente, elevar o nível de segurança digital. Além disso, a capacidade de configurar o dispositivo de acordo com os cargos predefinidos dos colaboradores nas organizações, diferencia o KIS das outras soluções que exigem processos manuais e morosos para a atribuição de acessos.

Background do Promotor

Enquanto promotor do KIS, possuo um perfil académico e profissional que integra competências relevantes para o desenvolvimento e implementação de soluções tecnológicas inovadoras na área da segurança digital. Sou licenciado em Gestão Empresarial e atualmente estou a realizar e a concluir o Mestrado de Negócio Eletrónico, o que me confere uma base sólida de conhecimento na área de gestão empresarial, estratégias digitais e inovação tecnológica. Adicionalmente, possuo uma vasta experiência profissional em análise de dados, área na qual desenvolvi competências analíticas e uma abordagem orientada para a tomada de decisões baseadas em dados concretos e factuais.

Atualmente, ocupo a posição de responsável de uma equipa de gestão de dados de fornecedores, função essa que implica uma forte capacidade de gestão de informações, coordenação de equipa e implementação de processos eficientes e automatizados em ambientes corporativos. A experiência adquirida ao longo da minha carreira em ambientes de análise de dados e gestão de equipas fornece-me uma visão sólida para a criação da solução KIS, de forma a garantir uma abordagem estratégica e orientada para a inovação no desenvolvimento de soluções de segurança.

MERCADO SUBJACENTE

A KIS, Lda. posiciona-se no mercado da segurança digital, um setor em expansão devido ao aumento das ameaças digitais e à crescente necessidade de soluções eficazes para proteger dados sensíveis e ativos digitais. A segurança digital tornou-se uma prioridade tanto para indivíduos como para empresas, em virtude da proliferação de ataques informáticos, roubo de identidade e da necessidade de proteger criptoativos. O mercado subjacente pode ser analisado a partir de diversas perspetivas, incluindo tendências, segmentação, concorrência, oportunidades e ameaças.

Segmentação de Mercado

B2C:

Profissionais da Área Financeira: Gestores de fundos de criptoativos, que necessitam de elevados padrões de segurança para realizar transações e armazenar ativos digitais. Estes profissionais estão cada vez mais expostos a ataques digitais e, portanto, requerem dispositivos de segurança avançados e multifuncionais.

Utilizadores Individuais Conscientes e/ou Inconscientes de Matéria de Segurança Online: Estes utilizadores podem estar mais ou menos informados sobre os riscos da segurança digital, mas procuram, em ambos os casos, formas de proteger as suas identidades, dados e ativos digitais. A dificuldade em gerir múltiplas palavras-passe leva à procura de soluções práticas, como a KIS, que integra a gestão de acessos de forma segura e simples.

B2B:

Empresas: Organizações que necessitam de proteger dados sensíveis e que enfrentam desafios na gestão de acessos devido à rotatividade de colaboradores e à integração de novos utilizadores. O KIS apresenta uma solução eficaz para a criação de acessos, ao permitir a sua personalização através da biometria, o que facilita a gestão e reforça a segurança digital das empresas.

Análise de Tendências do Mercado

A segurança digital tem sido uma área em constante evolução, impulsionada pelo aumento das ameaças e pela crescente dependência da tecnologia nas diversas esferas da vida. As principais tendências que impactam o mercado da segurança digital e a proposta do KIS, incluem:

Adoção de Tecnologias Biométricas: O uso de biometria, como impressões digitais, reconhecimento facial e íris, está a crescer de forma exponencial. Este tipo de autenticação é considerado o mais seguro e conveniente em comparação com as tradicionais palavras-passe. O mercado está a migrar cada vez mais para soluções baseadas em biometria devido à sua capacidade de oferecer uma experiência de uso mais simplificada, sem comprometer a segurança.

Aumento do Investimento em Criptoativos: Com o aumento do interesse em criptoativos e a sua integração em sistemas financeiros tradicionais, a proteção de ativos digitais tornou-se uma prioridade. Soluções de segurança como o KIS, que combinam autenticação biométrica e gestão de acessos, são altamente valorizadas neste setor.

Crescimento do Mercado de Identidade Digital: A gestão de identidades digitais é um campo emergente, com as organizações a adotarem soluções que integrem vários fatores de autenticação e controlo de acessos. A necessidade de garantir a privacidade e a segurança dos dados dos utilizadores está a aumentar, especialmente com a implementação do RGPD na União Europeia.

Cibersegurança como Prioridade Empresarial: As organizações estão a enfrentar um aumento significativo na frequência e sofisticação dos ataques virtuais. Como resposta, as empresas estão a investir em soluções de segurança integradas para proteger dados sensíveis e garantir a continuidade operacional.

Análise Competitiva

O KIS irá operar num mercado competitivo, com diversos concorrentes que oferecem soluções focadas em segurança e gestão de identidades digitais.

Os principais concorrentes podem ser agrupados em três categorias:

Empresas de Hardware de Segurança: Fabricantes como Ledger, Trezor, e Yubico dominam o mercado de dispositivos de segurança, ao oferecer soluções especializadas em proteção de chaves privadas e dados sensíveis. No entanto, estas soluções são frequentemente limitadas à proteção de criptoativos e não abordam outras áreas de segurança digital, como o controlo de acessos a sistemas corporativos.

Provedores de Software de Autenticação Multifatorial: Empresas como Authy, Okta e Duo Security oferecem soluções de autenticação multifatorial (MFA), muitas vezes focadas em ambientes corporativos. Estas soluções são amplamente utilizadas para reforçar a segurança em plataformas online, mas, em muitos casos, carecem da integração de diferentes funções de segurança num único dispositivo.

Plataformas de Armazenamento de Criptoativos: Empresas como Coinbase, Binance e Bitstamp dominam o mercado de troca e gestão de criptoativos. Embora estas plataformas se concentrem na segurança de transações financeiras digitais, as soluções que oferecem podem ser mais vulneráveis a ataques do que as soluções dedicadas exclusivamente à segurança do utilizador, como o KIS.

A principal vantagem competitiva do KIS reside na sua abordagem integrada, que combina a segurança de dados, a autenticação biométrica e a gestão de acessos e criptoativos num único dispositivo. A proposta do KIS visa não só a proteção de criptoativos, mas também a simplificação da gestão de acessos e identidades digitais em diversas plataformas, o que o distingue da maioria dos concorrentes.

Concorrentes

O KIS enfrenta concorrência de várias empresas estabelecidas no mercado de segurança digital, cada uma com uma proposta única de valor. Entre os principais concorrentes encontram-se a Mooltipass, a LastPass e a Ledger. Neste sentido, é crucial realizar uma análise comparativa e detalhada entre o KIS e esses concorrentes, na qual será analisado os seus pontos fortes, fracos e as principais diferenças.

Mooltipass

Produto: O Mooltipass é um dispositivo de hardware desenvolvido para gestão de palavras-passe e autenticação multifatorial. Ele armazena de forma segura os acessos do utilizador e facilita o acesso a plataformas online.

Vantagens:

Segurança de Hardware: O Mooltipass utiliza um dispositivo físico que armazena as palavras-passe de forma segura, isolando-as do ambiente digital, o que proporciona uma camada adicional de proteção.

Autonomia: Não depende de qualquer software instalado no computador ou em dispositivos móveis, o que o torna uma solução independente e resistente a ataques digitais.

Desvantagens:

Funcionalidade Limitada: Embora ofereça proteção de palavras-passe, a Mooltipass não integra outras funções de segurança, como a autenticação biométrica ou a gestão de criptoativos.

Menor Conveniência: O dispositivo é relativamente pequeno e pode ser de difícil utilização para alguns utilizadores, especialmente se for necessário inserir manualmente as credenciais.

Comparação com o KIS: O KIS oferece uma solução mais eficaz ao integrar autenticação biométrica e gestão de criptoativos, o que lhe confere uma vantagem em termos de multifuncionalidade e segurança. Além disso, o KIS oferece uma interface mais intuitiva, o que irá otimizar a experiência do utilizador, enquanto o Mooltipass é uma solução mais rígida e com menor flexibilidade.

LastPass

Produto: LastPass é uma plataforma de gestão de palavras-passe baseada em software, que armazena os acessos do utilizador na nuvem. Além de permitir o preenchimento automático de palavras-passe, oferece funcionalidades como autenticação multifatorial e a capacidade de partilhar credenciais de forma segura.

Vantagens:

Acessibilidade: Por ser baseada na nuvem, o LastPass permite o acesso através de qualquer dispositivo, o que facilita o uso para indivíduos que necessitam de aceder a informações em vários locais.

Funcionalidade Avançada: LastPass oferece funcionalidades adicionais, como o armazenamento de documentos seguros e a possibilidade de partilhar palavras-passe de forma controlada entre utilizadores.

Desvantagens:

Risco de Armazenamento na Nuvem: Apesar de utilizar criptografia forte, o armazenamento de palavras-passe na nuvem pode tornar o LastPass vulnerável a ataques se as credenciais de acesso forem comprometidas.

Dependência de Conexão à Internet: O LastPass requer uma conexão à internet para sincronizar os dados entre dispositivos, o que pode ser um inconveniente em caso de falhas na rede.

Comparação com a KIS: O KIS destaca-se por ser uma solução baseada em hardware e offline, o que reduz os riscos associados ao armazenamento em nuvem, como ataques e roubo de dados. Além disso, a integração da autenticação biométrica no dispositivo KIS proporciona uma camada de segurança adicional, algo que o LastPass não oferece, dado ser exclusivamente baseado em software.

Ledger

Produto: A Ledger é uma das empresas líderes no mercado de carteiras de hardware para armazenamento de criptoativos. A sua principal solução, a Ledger Nano, utiliza um dispositivo físico para proteger as chaves privadas de criptomoedas e garantir transações seguras.

Vantagens:

Segurança Avançada para Criptoativos: A Ledger utiliza um dispositivo de hardware que protege as chaves privadas do utilizador, o que a torna uma das soluções mais seguras para o armazenamento de criptoativos.

Suporte a Vários Criptoativos: A Ledger suporta uma ampla gama de criptomoedas, o que o torna uma opção popular entre os investidores de criptoativos.

Desvantagens:

Foco Exclusivo em Criptoativos: Embora seja altamente eficaz para proteger criptoativos, o Ledger não oferece uma solução abrangente para outras necessidades de segurança, como a gestão de acessos a sistemas ou autenticação biométrica.

Custo: O Ledger tem um custo mais elevado em comparação com soluções de software, devido à necessidade de um dispositivo físico.

Comparação com a KIS: O KIS compartilha com a Ledger o foco em segurança física, mas expande a sua proposta de valor para incluir a autenticação biométrica e a gestão de acessos, ao proporcionar uma solução mais ampla e integradora. Além disso, o KIS não se limita ao armazenamento de criptoativos, ao oferecer uma solução de segurança global que pode ser utilizada por qualquer utilizador ou empresa para proteger dados e identidades digitais.

Resumo Comparativo

Característica	KIS	Mooltipass	LastPass	Ledger
Tipo de Produto	Hardware biométrica + gestão de criptoativos (autenticação e gestão de palavras-passe)	Hardware (gestão de palavras-passe)	Software (gestão de palavras-passe na nuvem)	Hardware (armazenamento de criptoativos)
Segurança Física	Sim, via dispositivo e biometria	Sim, via dispositivo físico	Não, depende da nuvem	Sim, via dispositivo físico
Facilidade de Uso	Alta, com interface intuitiva	Moderada, com interface limitada	Alta, mas dependente da internet	Moderada, foco em criptoativos
Apoio Criptoativos	Sim, gestão integrada de criptoativos	Não	Não	Sim, foco exclusivo em criptoativos
Apoio Autenticação Multifatorial	Sim, via biometria e dispositivos	Não	Sim, via software	Não
Vulnerabilidades	Baixas, devido à segurança física	Moderadas, exposição a ataques físicos	Moderadas, vulnerabilidades na nuvem	Moderadas, limitado a criptoativos
Preço	Médio (280€)	Baixo a médio (140€)	Baixo (associação a subscrição – 3 a 6€/mês)	Alto (devido ao hardware especializado – 80 a 400€)

Tabela 1 - Comparação da Concorrência

Com base nesta análise comparativa, é possível perceber que o KIS se destaca pela sua abordagem multifuncional, que vai além da simples gestão de palavras-passe e oferece uma solução de segurança abrangente. A integração da autenticação biométrica e a proteção de criptoativos tornam a KIS uma opção mais completa e versátil, especialmente quando comparada com a Mooltipass, que se foca apenas na gestão de acessos, e com a Ledger, que é especializada em criptoativos, mas não oferece uma solução tão ampla para a segurança digital como um todo.

Oportunidades e Ameaças no Mercado

Oportunidades:

Crescimento do Mercado de Criptoativos: Com o aumento do interesse e da adoção de criptoativos, especialmente das moedas digitais descentralizadas, o KIS tem a oportunidade de se consolidar como uma solução de segurança essencial para a gestão e proteção desses ativos.

Aumento da Preocupação com a Privacidade e Segurança: O crescente interesse na privacidade digital e na implementação do RGPD criam uma forte procura por soluções de segurança que garantam a proteção dos dados pessoais. A KIS pode capitalizar esta tendência ao posicionar-se como uma solução que integra segurança e privacidade de forma eficiente.

Adoção Generalizada de Soluções de Identidade Digital: A digitalização de processos empresariais e a necessidade de soluções eficazes de gestão de identidades digitais oferecem à KIS uma oportunidade para expandir a sua oferta no mercado B2B, ao ajudar as empresas a integrar sistemas de segurança de acessos de forma simplificada.

Ameaças:

Concorrência Intensa: O mercado da segurança digital está altamente competitivo, com grandes empresas de tecnologia a desenvolverem soluções cada vez mais sofisticadas. O KIS deve continuar a inovar e a adaptar-se às mudanças para se manter competitivo.

Mudanças de Regulamentação: A evolução das regulamentações de segurança digital e da privacidade pode impor restrições à forma como a KIS opera, especialmente no que diz respeito ao tratamento de dados pessoais. A conformidade com as normativas internacionais será crucial para a operação do negócio.

Riscos da Evolução das Ameaças: A constante evolução das ameaças digitais, representa uma ameaça constante à eficácia das soluções de segurança existentes. O KIS terá de garantir que a sua solução se adapta continuamente a novas vulnerabilidades.

Expectativas de Crescimento e Projeções

O mercado da segurança digital está a crescer a um ritmo acelerado, com uma taxa de crescimento anual estimada em 10% até 2027, conforme indicado pela MarketsandMarkets (2024) no seu relatório sobre as tendências e previsões do setor de segurança digital. O KIS prevê um crescimento especulativo significativo, especialmente nos segmentos B2B e B2C, à medida que a procura por soluções de segurança integradas e acessíveis aumenta.

As projeções (especulativas) para os próximos cinco anos indicam:

Crescimento de Receita: Espera-se que a KIS atinja uma taxa de crescimento anual composta (CAGR) de 10% a 30% nos primeiros 3 anos, à medida que a solução ganha adoção no mercado B2B e entre utilizadores individuais. Valores meramente especulativos ao considerar como exemplo a taxa de crescimento da LastPass.

Expansão de Mercado: A estratégia de expansão inicial prevê a entrada no mercado europeu, com Portugal como país piloto, seguida pela expansão para regiões altamente digitalizadas e com uma crescente procura por tecnologias de autenticação biométrica e proteção de criptoativos (ex: Japão e Estados Unidos).

Rentabilidade: A empresa KIS tem como objetivo atingir a rentabilidade nos primeiros 3 anos de operação, com uma margem líquida superior a 20% a partir do terceiro ano, devido à crescente procura e à eficiência operacional proporcionada pela sua solução integrada (valores meramente especulativos).

A NOVA IDEIA E O SEU POSICIONAMENTO NO MERCADO

Descrição do Produto/Serviço e o seu Mercado

A KIS, Lda., uma sociedade por quotas com sede em Portugal, emerge como uma entidade inovadora no panorama tecnológico com foco em soluções de segurança digital.

A nossa principal missão é a conceção de ferramentas que enderecem a crescente problemática das ameaças virtuais, um desafio amplificado pela evolução constante da tecnologia e pela conseqüente proliferação de ataques digitais que comprometem a privacidade e a integridade dos dados dos utilizadores.

O dispositivo KIS (*Keep It Safe*) é uma solução transformadora da segurança digital que integra autenticação biométrica, gestão de acessos e de criptoativos num único dispositivo. O produto visa responder a duas das questões mais prementes no atual contexto digital: a proteção de dados e a gestão segura de acessos e criptoativos. O dispositivo KIS combina um sistema de autenticação biométrica com a capacidade de gerir múltiplos acessos e criptoativos de forma simplificada e segura. Ao utilizar tecnologia de impressão digital o dispositivo autentica o utilizador de maneira única, ao permitir aceder a serviços e realizar transações de forma rápida e sem necessidade de memorizar palavras-passe complexas.

Principais Funcionalidades:

Autenticação Biométrica: A solução utiliza tecnologia de leitura de impressões digitais, o que assegura que apenas o utilizador autorizado tenha acesso às informações sensíveis ou aos sistemas que requerem segurança adicional.

Gestão de Criptoativos: O dispositivo integra uma "carteira digital" para a gestão de criptoativos, como Bitcoin, Ethereum e outras criptomoedas, o que oferece aos utilizadores uma forma segura e sem complicações de aceder e transferir ativos digitais.

Gestão de Acessos: O KIS oferece uma solução eficaz e versátil para a gestão de acessos, adaptada tanto a utilizadores individuais como a organizações. Para os utilizadores particulares, permite substituir o uso de múltiplas palavras-passe por autenticação biométrica, o que irá simplificar o acesso a plataformas digitais de forma segura e conveniente. No contexto empresarial, o KIS possibilita a atribuição de permissões com base em funções ou cargos específicos, associando-as diretamente à impressão digital de cada colaborador.

Esta abordagem reduz a complexidade na criação e revogação de acessos, o que irá aumentar a eficiência operacional e reforçar a segurança no acesso a sistemas internos.

Proteção contra Fraudes: O dispositivo KIS irá incorporar mecanismos fundamentais de proteção, como a autenticação biométrica, o que limita o acesso apenas ao utilizador autorizado. Adicionalmente, prevê-se a implementação de uma camada extra de segurança através do envio de um PIN de ativação único para o contacto pessoal do utilizador (e-mail ou número de telemóvel), de forma a garantir que mesmo em caso de extravio físico, o dispositivo permaneça inacessível a terceiros. Estes elementos asseguram uma base sólida de proteção contra acessos não autorizados, ao reforçar a privacidade e a confiança na utilização do KIS.

Compatibilidade com Sistemas de Segurança Existentes: O KIS será desenvolvido para se integrar facilmente com as infraestruturas de segurança digital já existentes. A sua flexibilidade e compatibilidade tornam-no numa solução adaptável para diferentes tipos de utilizadores e organizações.

Utilização e Simplicidade: A interface do dispositivo será concebida para ser intuitiva, sem comprometer a complexidade das funções de segurança. O utilizador irá apenas precisa de registar a sua impressão digital e, a partir daí, o dispositivo gere automaticamente os acessos e transações.

O dispositivo KIS será projetado para atender a dois segmentos principais:

B2C (Business-to-Consumer): Indivíduos preocupados com a proteção dos seus dados pessoais e ativos digitais, como profissionais da área financeira e utilizadores gerais que enfrentam desafios com a gestão de múltiplas palavras-passe e desejam uma solução integrada e segura.

B2B (Business-to-Business): Empresas que necessitam de uma solução eficiente para a gestão de acessos dos seus colaboradores, especialmente em contextos de elevada rotatividade de recursos-humanos ou com necessidade de proteger grandes volumes de dados sensíveis.

O produto será posicionado como uma solução de alta segurança, baseada em tecnologia biométrica avançada, que simplificará a experiência do utilizador, ao mesmo tempo que oferece um nível elevado de proteção digital.

Visão, Missão e Valores do KIS

Visão

Ser a referência global em soluções de segurança digital e gestão de criptoativos, ao promover um ecossistema seguro, eficiente e acessível para indivíduos e organizações. A nossa visão consiste em redefinir a cibersegurança através da inovação contínua, ao assegurar a integridade e proteção dos dados dos nossos clientes.

Missão

Desenvolver e fornecer soluções tecnológicas avançadas que garantam a segurança digital, ao combinar autenticação biométrica, criptografia eficaz e de utilização intuitiva. O KIS compromete-se a criar produtos que simplifiquem a proteção de criptoativos e dados sensíveis, de forma a garantir a conformidade regulatória e maximizar a confiança dos utilizadores no ambiente digital.

Valores

1. Segurança – Comprometemo-nos a desenvolver soluções que assegurem a máxima proteção dos dados dos nossos clientes.

2. Inovação – Investiremos na pesquisa e desenvolvimento para oferecer soluções tecnologicamente avançadas.

3. Confiança – Promovemos transparência e fiabilidade nos nossos produtos e serviços.

4. Utilização – Criamos interfaces intuitivas que facilitarão a experiência do utilizador sem comprometer a segurança.

5. Ética – Atuamos em conformidade com as normas reguladoras e princípios éticos da cibersegurança.

6. Sustentabilidade – Desenvolvemos soluções eficientes que minimizam o impacto ambiental e maximizam a longevidade dos dispositivos.

7. Excelência – Procuramos constantemente a melhoria contínua para fornecer produtos e serviços de elevada qualidade.

Marketing Mix (8 Ps) do KIS

1. Produto (*Product*)

O KIS é um dispositivo de segurança digital que combina autenticação biométrica com a gestão de criptoativos. As suas principais características irão incluir:

- Autenticação Biométrica – Garantia de acesso exclusivo através de impressão digital e multifatorial.
- Criptografia Avançada – Proteção de informações sensíveis contra acessos não autorizados.
- Armazenamento Seguro – Mecanismo de segurança offline para guardar chaves privadas de criptoativos.
- Integração Multiplataforma – Compatibilidade com diversos dispositivos e sistemas operativos.
- Design Ergonómico e Durável – Materiais resistentes e com formato compacto para facilitar o transporte e a utilização.

2. Preço (*Price*)

A política de preços do KIS irá basear-se num modelo de valor agregado, ao considerar os seguintes fatores:

- Preço Premium Justificado – Devido à tecnologia inovadora e à elevada segurança proporcionada pelo dispositivo.
- Estratégia de Preço Adaptada – Futuramente existirá uma diferenciação entre versões “Light” e premium, ao oferecer funcionalidades adicionais mediante um custo superior.
- Modelo de Subscrição – Possibilidade de serviços especializados e condições específicas através de uma assinatura mensal ou anual.
- Descontos para Empresas e Instituições – Políticas especiais para clientes corporativos e parceiros estratégicos.

3. Distribuição (*Place*)

A estratégia de distribuição do KIS assenta numa abordagem multicanal, ao combinar pontos de contacto digitais e físicos para maximizar o alcance e a acessibilidade:

- **Website Institucional com Informação Comercial:** Inicialmente, será criado um site institucional que apresentará o produto e indicará os canais de aquisição disponíveis (lojas físicas, marketplaces, entre outros).
- **Marketplaces Digitais e Especializados:** O dispositivo estará disponível em plataformas de venda online com forte presença no setor tecnológico, como a Amazon, a FNAC online, a Worten online e outros marketplaces reconhecidos.
- **Parcerias com Revendedores e Integradores de Soluções:** Serão estabelecidas parcerias com empresas de cibersegurança e revendedores tecnológicos especializados, com foco na venda em contexto empresarial.
- **Participação em Eventos do Setor:** O KIS será promovido e comercializado em feiras e eventos relevantes da área tecnológica e de segurança digital (por exemplo, Web Summit), de forma a potenciar a visibilidade e o contacto direto com os potenciais utilizadores.

4. Promoção (*Promotion* - Comunicação e Publicidade)

A estratégia de comunicação do KIS envolverá:

- **Marketing Digital – Campanhas** direcionadas em redes sociais, SEO e anúncios pagos.
- **Parcerias com Influenciadores e Especialistas – Colaboração** com profissionais do setor para credibilização da marca.
- **Demonstrações e Webinars – Sessões** informativas sobre a importância da segurança digital e a utilidade do KIS.
- **Publicações Científicas e Estudos de Caso – Divulgação** em revistas e blogs especializados.

5. Pessoas (*People*)

A equipa do KIS será composta por perfis especializados nas áreas de cibersegurança, desenvolvimento de produto, gestão e direito empresarial. Numa fase inicial, o foco estará nas competências essenciais à validação do modelo de negócio, prevenindo-se a expansão progressiva da estrutura consoante as exigências do projeto. A formação contínua e a orientação para a segurança digital e satisfação do cliente serão pilares da atuação da equipa.

6. Processos (*Process*)

A eficiência operacional do KIS irá basear-se em processos otimizados, como:

- Investigação e Desenvolvimento (I&D) – Melhoria contínua das tecnologias implementadas.
- Testes de Segurança Rigorosos – Avaliação contínua de vulnerabilidades e atualizações de software.
- Consultoria digital – Assistência célere e eficaz em matéria de segurança digital e correta utilização do dispositivo.

7. Provas Físicas (*Physical Evidence*)

Para fortalecer a credibilidade do KIS, serão utilizados elementos tangíveis e intangíveis, tais como:

- Certificações de Segurança – Como por exemplo o ISO 27001 e GDPR.
- Design e Embalagem “*Premium*” – Um produto visualmente atrativo que transmite sofisticação e segurança. Esta incluirá um selo inviolável exclusivo do KIS, cuja integridade permite detetar qualquer tentativa de adulteração, garantindo que o dispositivo chega intacto e protegido ao utilizador final.
- Testemunhos e Casos de Sucesso – Relatos de clientes satisfeitos e demonstrações da eficácia do dispositivo.

8. Produtividade e Qualidade (*Productivity & Quality*)

O KIS irá comprometer-se com elevados padrões de qualidade, ao garantir:

- Produção Sustentável – Redução de impacto ambiental na escolha de materiais e processos de fabrico.
- Eficiência Operacional – Minimização de custos e otimização de recursos para oferecer um produto competitivo.
- Garantia de Satisfação – Política de devolução e plano de subscrição para assegurar a confiança dos consumidores.

Recursos Físicos e de Produção Necessários

Para garantir a produção e distribuição eficaz do dispositivo KIS, será necessário recursos físicos e de produção específicos desde a fabricação do hardware até ao desenvolvimento contínuo do software, assim como uma eficiente gestão da cadeia de distribuição. Os principais recursos e parceiros necessários para garantir a viabilidade e o sucesso do projeto são os seguintes:

Fornecedores e Parcerias

A produção do dispositivo KIS será assegurada através de parcerias com fabricantes especializados em hardware de segurança digital e tecnologias de autenticação. A KIS, Lda. pretende estabelecer colaborações estratégicas com fornecedores de componentes eletrónicos de alta segurança, como microcontroladores, sensores biométricos, módulos de comunicação (NFC, Bluetooth) e unidades de armazenamento criptografado. Estes componentes serão selecionados com base na sua conformidade com as normas internacionais de cibersegurança e no histórico de fiabilidade em aplicações críticas.

A produção será escalável, de forma a permitir ajustar a capacidade à evolução da procura e à introdução progressiva do produto nos segmentos B2C e B2B.

Em termos geográficos, será dada preferência a mercados tecnologicamente maduros e com estruturas de produção consolidadas, como Alemanha, Suécia, Taiwan e Índia, dependendo do tipo de componente e da relação custo-qualidade.

No caso do armazenamento seguro de criptoativos, serão procuradas soluções baseadas em “Secure Elements” (elementos seguros), bem como infraestruturas de firmware com suporte e atualização contínua de segurança. A definição dos fornecedores será objeto de revisão constante, de forma a acompanhar a evolução tecnológica e as necessidades estratégicas do negócio.

Estas parcerias irão garantir que o dispositivo KIS tenha todas as funcionalidades de segurança necessárias para se destacar no mercado, ao combinar biometria avançada, gestão de identidades digitais e armazenamento seguro de criptoativos.

Distribuição

A estratégia de distribuição do dispositivo KIS assenta num modelo multicanal, com foco inicial na presença digital e na utilização de canais já estabelecidos no ecossistema tecnológico. A comercialização será promovida através de uma plataforma institucional própria, onde estarão disponíveis todas as informações relevantes sobre o produto, incluindo locais de venda, funcionalidades, perguntas frequentes e suporte ao cliente. Nesta fase, não será desenvolvida de imediato uma loja de e-commerce própria, em vez disso, a KIS privilegiará a presença em marketplaces digitais especializados, como a Worten Online ou outros canais de comércio eletrónico reconhecidos, o que permitirá reduzir custos operacionais e aumentar a visibilidade inicial do produto junto dos públicos-alvo.

Paralelamente, serão estabelecidas parcerias com retalhistas tecnológicos físicos, tais como FNAC, Worten, MediaMarkt e outras lojas especializadas em tecnologia e segurança digital, de forma a permitir alcançar utilizadores que privilegiam a compra presencial e aumentar a confiança de segmentos mais conservadores. Estes pontos de venda poderão também funcionar como canais de demonstração e teste do dispositivo, o que reforçará a perceção de valor do produto.

No que diz respeito à logística de distribuição, a KIS recorrerá a operadores de transporte experientes, como CTT, DHL, FedEx ou NACEX, cuja escolha será realizada de acordo com a região geográfica do consumidor final. Esta abordagem permitirá garantir uma entrega segura, eficiente e rastreável, ao assegurar o cumprimento dos prazos de envio e a integridade da embalagem.

Para mitigar os receios relacionados com a segurança na entrega, especialmente devido à natureza sensível do dispositivo, será incluído um selo de proteção inviolável nas embalagens, que sinalizará qualquer tentativa de violação antes da receção pelo cliente. Esta medida visa reforçar a confiança na integridade do produto e salvaguardar a reputação da marca. Para reforçar a segurança na ativação, o dispositivo exigirá ainda um código PIN de primeiro acesso, gerado unicamente para o cliente no momento da compra e enviado de forma segura (via e-mail ou mensagem para o telemóvel). Esta camada adicional garante que mesmo em caso de interceção física do dispositivo, o seu uso permanece bloqueado até ser ativado pelo comprador legítimo, o que aumentará substancialmente a confiança no canal de distribuição online.

Assim, a estratégia de distribuição do KIS reflete um equilíbrio entre presença digital e física, ao garantir flexibilidade na abordagem ao mercado e ajustando-se às preferências dos diferentes perfis de utilizador.

Capacidade de Gestão do Negócio dos Promotores

A equipa de gestão é um dos principais pilares para o sucesso da KIS, Lda. O fundador da empresa possui formação académica e experiência prática, que combina conhecimentos em gestão de negócios e tecnologia digital, essenciais para a liderança de um projeto inovador e de elevado risco.

- **Formação Académica e Experiência:** O fundador é licenciado em Gestão e encontra-se a concluir um mestrado em Negócio Eletrónico, com uma vasta experiência na análise de dados e gestão de equipas, sendo atualmente Team Leader de uma equipa de *Supplier Master Data*. Esta formação e experiência em análise de dados, aliadas ao domínio dos conceitos de segurança digital e inovação tecnológica, são cruciais para a implementação e o sucesso do projeto.

- **Capacidade de Tomada de Decisão e Gestão de Riscos:** O terá de demonstrar uma sólida capacidade de tomar decisões estratégicas e de gestão, Competências que terá adquirido ao trabalhar em ambientes internacionais e desafiantes, onde a adaptabilidade e a capacidade de identificar oportunidades e mitigar riscos são fundamentais.

- **Visão e Compromisso:** A equipa estará profundamente comprometida com a missão de transformar a KIS numa referência de segurança digital e gestão de acessos, com uma visão clara de expansão para o mercado de criptoativos e soluções empresariais.

Sumário dos Executivos e Experiências Relevantes

A equipa fundadora será composta por executivos com uma vasta experiência na gestão empresarial, na área de segurança digital e em inovação tecnológica:

Omar Soares – CEO e Fundador

- **Formação:** Licenciado em Gestão Empresarial, Mestrado em Negócio Eletrónico.
- **Experiência:** Experiência sólida em gestão de equipas e análise de dados, com destaque para o cargo atual de Team Leader na empresa Infineon.
- **Contribuições Relevantes:** Liderança de equipa em ambientes de alta exigência, gestão de processos complexos e desenvolvimento de soluções inovadoras.

Sócio Especialista em Software

- **Formação:** Licenciado em Engenharia Informática, Mestrado em Desenvolvimento de Software e Inteligência Artificial.
- **Experiência:** Mais de 6 anos de experiência em desenvolvimento de software e integração de sistemas, com especialização em segurança digital e autenticação biométrica.
- **Contribuições Relevantes:** Desenvolvimento de soluções de software seguras e escaláveis, com foco em inovação e facilidade de utilização. Liderança de projetos técnicos e implementação de sistemas complexos em empresas internacionais, de forma a garantir a qualidade e segurança dos produtos.

Sócio Especialista na Área Jurídica:

- Formação: Licenciado em Direito, Pós-graduação em Direito da Tecnologia e Proteção de Dados.
- Experiência: Advogado especializada em direito digital, privacidade e proteção de dados pessoais, com mais de 5 anos de experiência em assessoria jurídica para startups de tecnologia e empresas de segurança digital.
- Contribuições Relevantes: Consultoria jurídica em questões de conformidade com regulamentos internacionais de proteção de dados, como o GDPR, e a elaboração de políticas de segurança e privacidade para plataformas digitais. Especialização em contratos e licenciamento de software.

Sócio Especialista em Design de Produto

- Formação: Licenciado em Design de Produto, Mestrado em Design de Interação e Experiência do Utilizador.
- Experiência: 5 anos de experiência na criação de interfaces e produtos inovadores, com foco em segurança, acessibilidade e design centrado no utilizador. Experiência com design de hardware e software para dispositivos de autenticação biométrica e dispositivos de segurança digital.
- Contribuições Relevantes: Desenvolvimento de produtos intuitivos e de fácil utilização, com ênfase na experiência do utilizador e na integração de segurança sem comprometer a funcionalidade. Gestão de processos de design e prototipagem de novos produtos, garantindo a inovação e a competitividade no mercado.

Cada um dos membros da equipa fundadora traz um conjunto único de habilidades e experiências que permitirão à KIS oferecer soluções inovadoras e de alta qualidade no campo da segurança digital, autenticação biométrica e gestão de criptoativos.

Estatuto Legal do Negócio – Forma Jurídica

De acordo com a legislação em vigor (2025) referente às formas jurídicas, legisladas através do Código das Sociedades Comerciais, a empresa KIS, Lda. será registada como uma Sociedade por Quotas.

O modo de constituição será através do modelo “Empresa Online”, regulado no Decreto-Lei n.º 125/2006, de 29 de junho, com as alterações subsequentes até ao Decreto-Lei n.º 109-D/2021, de 9 de dezembro, e também na Portaria n.º 657-C/2006, de 29 de junho.

Foi optado por o modelo “Empresa na hora”, uma vez que vai de acordo com os princípios de uma empresa direcionada para o mercado digital. Outro dos motivos foi a facilidade de criação de empresa através deste modelo, sendo que o tempo médio de abertura através deste modelo é de apenas 48 minutos.

Para a abertura da empresa vamos ter o custo inicial de 220 € pois foi optado por se realizar o pacto social pré-aprovado. O valor referente ao Capital Social vai ser depositado pelos sócios no final do primeiro exercício económico.

Patentes

Para salvaguardar o dispositivo KIS, optou-se por utilizar uma patente de invenção que se encontra atualmente em fase de desenvolvimento, uma vez que é a forma mais ampla de proteger legalmente uma invenção contra fabrico, oferta, armazenamento, introdução no comércio ou utilização indevidas. O produto fica protegido por um período máximo de 20 anos, contados a partir da data do pedido.

Para criar a patente, foram considerados os seguintes custos:

- Resposta a notificação (com ou sem alteração de reivindicações, descrição, desenhos, resumo, epígrafe ou outros elementos) – 27,27€
- Pedido – 109,07€
- Pedido de licença de exploração obrigatória – 10,91€
- Custos manutenção – são apenas a ter em conta a partir do 5º ano de utilização

Organigrama da Empresa

A KIS, Lda. será uma empresa composta por uma equipa de sócios com competências complementares, na qual cada um será responsável por uma área-chave da operação e desenvolvimento do produto. O organigrama da empresa será estruturado da seguinte forma:

1. CEO e Fundador – Omar Soares

- Responsável pela gestão geral da empresa, estratégia de negócios, desenvolvimento e implementação de objetivos de longo prazo e supervisão de todas as operações da empresa.
- O CEO será o principal responsável pela gestão da equipa, gestão de financiamentos e relações com investidores.

2. Sócio Especialista em Software – A definir

- Responsável pelo desenvolvimento do software de gestão de acessos e criptoativos, incluindo a integração de autenticação multifatorial e segurança digital.
- Irá coordenar a equipa técnica de desenvolvimento e supervisionar a evolução do software em conformidade com as necessidades do mercado e novas ameaças de segurança.

3. Sócio Especialista na Área Jurídica - A definir

- Responsável pela gestão de conformidade legal, incluindo proteção de dados, direitos de propriedade intelectual, contratos empresariais e regulamentação de segurança digital.
- Irá garantir que a KIS, Lda. esteja em total conformidade com as normas e regulamentações locais e internacionais, como o Regulamento Geral de Proteção de Dados (RGPD) e outras legislações pertinentes.

4. Sócio Especialista em Design de Produto - A definir

- Responsável pelo desenvolvimento e atualização do hardware do dispositivo KIS, incluindo a conceção de dispositivos que atendam aos mais elevados padrões de segurança física e facilidade de utilização.

- Irá liderar o processo de design de produto, incluindo a seleção de componentes de hardware e a criação de protótipos, além de supervisionar as parcerias com fabricantes e fornecedores especializados.

Objetivos da Empresa

Os principais objetivos da KIS, Lda. são:

1. Desenvolver e Comercializar o Produto KIS: Lançar o dispositivo de segurança digital no mercado, inicialmente com foco nos segmentos B2C e B2B, e expandir gradualmente para novas funcionalidades.

2. Atingir a Sustentabilidade Financeira: Gerar receitas consistentes através da venda de dispositivos e serviços associados, para garantir uma margem de lucro saudável e um crescimento sustentável no mercado global.

3. Inovação Contínua: Continuar a desenvolver novas funcionalidades e melhorar a experiência do utilizador, com foco na segurança e na adaptação às novas ameaças digitais que surgem.

4. Expansão Global: Expandir a operação para mercados internacionais, com foco em países da União Europeia e, posteriormente, para mercados fora da região.

A KIS, Lda. apresenta-se como uma empresa empreendedora, com um produto inovador e uma equipa de gestão experiente, pronta para enfrentar os desafios do mercado de segurança digital. O projeto oferece uma solução única e avançada que responde à crescente preocupação com a segurança dos dados pessoais e ativos digitais. A equipa está bem posicionada para implementar este plano de negócios com sucesso, mostrando-se capaz de transformar esta ideia numa realidade rentável e sustentável.

O PROJETO / PRODUTO / IDEIA

Resumo do Projeto e Sumário das Atividades a Serem Desenvolvidas



Figura 3 - Logo KIS

O projeto KIS, Lda. visa o desenvolvimento de um dispositivo inovador que combina autenticação biométrica e gestão de criptoativos em uma solução integrada de segurança digital. O produto, denominado KIS (*Keep It Safe*), destina-se a fornecer uma forma segura e eficiente de gerenciar acessos e criptoativos, ao abordar a crescente problemática das ameaças digitais e das dificuldades associadas ao armazenamento seguro de dados e acessos.

Neste momento, o KIS encontra-se em estágio de prototipagem inicial. As primeiras funcionalidades básicas foram delineadas, como a integração da autenticação biométrica, com a gestão de acessos, e a conceção de um sistema que permita a sincronização e a associação de dispositivos para a autenticação e gestão de criptoativos.

As atividades a serem desenvolvidas para o lançamento do produto incluem:

- Desenvolvimento e Integração do Software: Criação da plataforma de gestão de acessos e criptoativos, que incluía autenticação multifatorial e integração com dispositivos de hardware.
- Desenvolvimento do Hardware: Melhorar o design do dispositivo KIS, com foco na segurança e facilidade de utilização, em colaboração com os parceiros de design de produto.
- Testes de Segurança e Uso: Avaliação da eficácia do dispositivo e da plataforma em termos de segurança, desempenho e experiência do utilizador.
- Licenciamento e Patentes: A empresa irá recorrer a proteção legal do produto por meio de patentes e licenças, com especial atenção para a proteção das inovações relacionadas à segurança biométrica e gestão de criptoativos.

Pontos Críticos no Desenvolvimento do Projeto

O desenvolvimento do KIS apresenta diversos desafios que exigem cuidados especiais e planeamento. Os principais pontos críticos incluem:

1. Integração do Software com o Hardware: A sincronização eficiente entre o software de gestão de acessos e o dispositivo de hardware será um desafio técnico significativo. A complexidade da integração de autenticação biométrica e criptoativos pode resultar em problemas de compatibilidade ou de desempenho que exigem atenção especializada.

2. Segurança do Sistema: A segurança do dispositivo será um ponto crítico, especialmente ao considerar a natureza sensível dos dados manipulados (acessos e criptoativos). A implementação de medidas de segurança eficaz será crucial para garantir a confiança do mercado.

3. Fornecedores e Parcerias: A dependência de fornecedores para componentes chave, como sensores biométricos e chips de segurança, pode impactar os prazos de entrega. A falta de flexibilidade ou problemas logísticos com os fornecedores podem prejudicar o lançamento do produto. Parcerias bem definidas e outros fornecedores serão cruciais para garantir a continuidade do fornecimento de componentes essenciais.

4. Regulamentações e Conformidade: A conformidade com a Regulamentação Geral de Proteção de Dados (RGPD) e outras normas internacionais será essencial para garantir a legalidade do produto, principalmente no que diz respeito à gestão de dados sensíveis e à privacidade do utilizador.

5. Testes e Certificação: O dispositivo passará por rigorosos testes de segurança e utilização para garantir que atenda aos padrões exigidos pelo mercado. A obtenção de certificações de segurança será um passo fundamental para estabelecer a confiança do mercado e a conformidade legal.

Motivação e Objetivos dos Intervenientes no Processo

A motivação dos intervenientes no projeto é impulsionada pelo desejo de oferecer uma solução inovadora para a crescente problemática das ameaças digitais. Cada sócio contribui com um conjunto único de competências e experiências que irá colaborar para o sucesso do projeto:

- **CEO e Fundador:** Motivado pela necessidade de resolver desafios de segurança digital e pela vontade de criar uma empresa que ofereça soluções inovadoras para proteger dados e identidades.

- **Especialista em Software:** Motivado pela possibilidade de desenvolver uma plataforma inovadora, eficaz na gestão de acessos e de criptoativos, que incorpore as mais recentes inovações em segurança digital.

- **Especialista Jurídico:** Motivado pela oportunidade de trabalhar num produto altamente regulado e desafiante, de forma a garantir conformidade com as leis de privacidade e segurança de dados.

- **Especialista em Design de Produto:** Motivado pela criação de um dispositivo seguro, funcional e esteticamente agradável, com foco na ergonomia e uso, para melhorar a experiência do utilizador.

Cada sócio tem um nível de envolvimento definido nas atividades do projeto, com um compromisso claro com os objetivos e uma compreensão das responsabilidades individuais no sucesso do empreendimento.

Tempo e Recursos Necessários para o Lançamento

O tempo estimado para o desenvolvimento completo do KIS é de 18 a 24 meses, considerando as fases de desenvolvimento, testes e obtenção de certificações. Durante este período, será necessário alocar os seguintes recursos:

- **Equipa Técnica:** Programadores de software, engenheiros de hardware e especialistas em segurança digital.

- **Infraestruturas de Produção:** Parcerias com fabricantes de hardware especializados para produção e montagem do dispositivo.

- **Testes de Qualidade e Certificação:** Contratação de empresas de segurança independentes para realizar auditorias e testes de qualidade no dispositivo e software.

- **Marketing e Estratégia de Lançamento:** Planeamento e execução de campanhas de marketing para promover o lançamento do produto e garantir uma receção positiva no mercado.

Produto / Serviço

O "KIS" (*Keep It Safe*) é um dispositivo desenvolvido para a gestão de credenciais de acesso e ativos criptográficos, com foco na segurança e facilidade de utilização.

O produto integra tecnologia avançada, que proporcionará uma solução eficaz e intuitiva para os utilizadores que necessitam de um elevado nível de proteção para dados e acessos digitais. Destaca-se pela utilização de autenticação biométrica baseada em impressão digital, que assegura o acesso exclusivo ao dispositivo, e pela combinação de conectividades USB-C e Near Field Communication (NFC), que conferem flexibilidade e versatilidade de integração com diferentes sistemas operativos e ambientes tecnológicos.

O dispositivo é fornecido com uma configuração padrão que inclui 1 TB de capacidade de armazenamento offline.

Será também implementado um plano de suporte evolutivo ao produto, com funcionalidades que acrescentem valor de forma prática e operacional através de pagamentos em prestações mensais ou anuais, que incluem:

- Acesso ao dispositivo.
- Troca direta do dispositivo em caso de lançamento de versões mais avançadas, o que permitiria ao cliente manter-se tecnologicamente atualizado.
- Substituição imediata do equipamento em caso de avaria.
- Serviço de consultoria em segurança digital, com recomendações de boas práticas, configurações e orientações personalizadas.
- Acesso prioritário a atualizações críticas e funcionalidades experimentais.

Esta flexibilidade funcional irá permitir ao utilizador adaptar o dispositivo às suas necessidades de segurança e gestão ao longo do tempo, conferindo-lhe maior autonomia, escalabilidade e controlo sobre os seus acessos e ativos digitais.

Proposta Única de Valor

O KIS oferece uma gestão de acessos e criptoativos mais segura e acessível do que as soluções tradicionais no mercado. A autenticação biométrica com impressão digital e PIN de desbloqueio (em caso de falha de leitura biométrica) serão a única forma de desbloqueio, o que confere um elevado nível de privacidade e exclusividade ao dispositivo.

Além disso, o seu design compacto e portátil, aliado à resistência de impactos e impermeabilidade, torna-o adequado para diversas situações de uso, incluindo ambientes externos.

Classificação do Produto

O KIS pode ser categorizado como um produto "Push" (método de promoção onde os produtos são apresentados ao consumidor através de canais de distribuição, como lojas), por meio de incentivos, promoções e publicidade direcionada a intermediários, visto que surge da inovação tecnológica, com base em pesquisa e desenvolvimento intensivos.

Embora exista uma procura crescente por soluções de segurança digital, o KIS introduz uma aplicação inédita para a gestão de credenciais e criptoativos, com uma proposta distinta em relação às soluções existentes no mercado.

Produção

A produção do dispositivo KIS será realizada através de uma combinação de processos internos e subcontratação estratégica a fornecedores especializados. Optamos por uma estratégia de produção híbrida para maximizar a flexibilidade e reduzir os custos iniciais de investimento em infraestrutura.

A subcontratação será realizada a empresas com experiência na produção de componentes eletrônicos e dispositivos de segurança digital, de forma a garantir a mais alta qualidade dos produtos e a eficiência dos processos de fabricação.

Maquinaria e Equipamentos Necessários

A produção do dispositivo KIS exigirá vários equipamentos especializados, incluindo máquinas de soldagem de alta precisão, sistemas de teste para componentes eletrônicos, sistemas de calibração para sensores biométricos e máquinas para a produção de moldes para as caixas do dispositivo.

Os principais equipamentos necessários incluem:

- **Máquinas de soldagem automática:** Para a montagem precisa dos circuitos eletrônicos nos dispositivos. Estimamos um investimento de 50.000€ para a aquisição de uma linha de soldagem de alta precisão.

- **Máquinas de calibração e teste de biometria:** Necessárias para calibrar e testar os sensores biométricos (impressão digital, reconhecimento facial e íris). O custo estimado dessas máquinas é de 40.000€.

- **Máquinas de embalagem automatizada:** Para garantir uma embalagem eficiente e de alta qualidade, com custos aproximados de 20.000€.

A aquisição desses equipamentos será realizada ao longo do primeiro ano de operação, com a possibilidade de expansão conforme a demanda de produção aumente.

Processo Produtivo

O processo produtivo será estruturado em várias fases, cada uma crítica para garantir a qualidade e a funcionalidade do dispositivo KIS. Para a respetiva simulação, serão apresentados valores meramente especulativos dado a fase de desenvolvimento em que o dispositivo se encontra.

1. Aquisição de Componentes: A primeira etapa envolve a aquisição de todos os componentes necessários para a produção, que incluem chips, sensores biométricos, módulos de criptografia e as carcaças do dispositivo.

Os principais fornecedores serão:

- Sensores Biométricos: O custo de cada módulo é de 25€ e a previsão de fornecimento para a produção inicial de 10.000 unidades é de 250.000€.
- Chips de Criptografia: O custo de cada chip será de 15€, com um fornecimento inicial de 150.000€ para a produção das primeiras 10.000 unidades.
- Carcaças e Componentes de Montagem: O custo estimado para a produção das primeiras 10.000 unidades é de 100.000€.

2. Montagem: Após a recepção dos componentes, a montagem será realizada por uma empresa especializada em produção eletrônica, como por exemplo a Jabil Inc., que tem experiência em montagem de dispositivos de alta precisão. A subcontratação da montagem e integração dos componentes terá um custo estimado de 20€ por unidade, totalizando 200.000€ para a produção inicial de 10.000 unidades.

3. Testes de Qualidade e Segurança: Cada dispositivo passará por uma série de testes rigorosos para garantir que os sensores biométricos e os módulos de criptografia funcionem corretamente. Isso inclui testes de precisão dos sensores biométricos, testes de segurança dos chips de criptografia e verificações de integridade do sistema. O custo de testes será de 5€ por unidade, ou 50.000€ para as primeiras 10.000 unidades.

4. Embalagem e Envio: Após a montagem e os testes, os dispositivos serão embalados em caixas personalizadas para proteção durante o transporte. A embalagem incluirá um manual de instruções e informações sobre segurança. O custo da embalagem é estimado em 2€ por unidade, com um custo total de 20.000€ para a produção inicial de 10.000 unidades.

Custos de Produção

A produção inicial de 10.000 unidades do dispositivo KIS terá os seguintes custos aproximados:

- Matérias-primas: 500.000€ (sensores biométricos, chips de criptografia, componentes de montagem)
- Montagem: 200.000€ (subcontratação da montagem e integração)
- Testes de Qualidade: 50.000€
- Embalagem: 20.000€

O total estimado para a produção das primeiras 10.000 unidades é de 770.000€.

Matéria-prima e Fornecedores

A produção do dispositivo KIS será viabilizada através da seleção de fornecedores com empresas especializadas na área do hardware dedicado à segurança digital e tecnologias de autenticação. A KIS, Lda. tem como objetivo estabelecer colaborações estratégicas com fornecedores de componentes eletrónicos altamente seguros, incluindo microcontroladores, sensores biométricos, módulos de e unidades de armazenamento com encriptação avançada. A seleção destes componentes será orientada pela sua conformidade com normas internacionais de cibersegurança e pela sua fiabilidade comprovada em contextos críticos.

Do ponto de vista geográfico, serão privilegiados mercados com elevada maturidade tecnológica e cadeias de produção consolidadas, como a Alemanha, Suécia, Taiwan e Índia. A escolha de fornecedores terá em conta o equilíbrio entre qualidade, inovação e competitividade de custos, consoante o tipo de componente a adquirir.

A definição e gestão dos fornecedores será objeto de análise contínua, com vista à constante adaptação às inovações tecnológicas e aos objetivos estratégicos do projeto.

Estas colaborações irão permitir que o KIS seja desenvolvido com os mais elevados padrões de segurança, ao reunir num único dispositivo a autenticação biométrica avançada, a gestão segura de identidades digitais e o armazenamento protegido de ativos criptográficos, assegurando assim uma proposta de valor diferenciadora no mercado.

Tempo de Entrega

O tempo de entrega após a receção da ordem de compra para os dispositivos dependerá diretamente da localização geográfica do cliente, contudo o prazo máximo espectável será de aproximadamente 30 dias úteis. Este prazo abrange a montagem, os testes de qualidade e o envio dos dispositivos em caso de falha de inventário.

A KIS, Lda. implementará um sistema de gestão de produção eficiente para garantir que todos os processos, desde a aquisição de matérias-primas até a entrega final ao cliente, sejam cumpridos dentro dos prazos estabelecidos.

Controle de Produção

A produção será controlada de forma a garantir a consistência e a qualidade do produto final. O nível de inventário será monitorado em tempo real, com um sistema de gestão integrado para acompanhar os materiais e componentes necessários para a produção contínua. A matéria-prima será adquirida de fornecedores estratégicos, com contratos de longo prazo para garantir preços competitivos e prazos de entrega consistentes.

Mecanismos de Controle de Produção

1. Gestão de inventários: Utilização de software de gestão de inventário para monitorizar os níveis de materiais e componentes.

2. Teste de qualidade: Implementação de um sistema de controle de qualidade rigoroso para garantir que todos os dispositivos atendem aos requisitos de segurança e desempenho.

3. Gestão de fornecedores: Relação estreita com fornecedores de componentes críticos, como o sensor biométrico e a bateria, com acordos de fornecimento contínuo para garantir a disponibilidade e a qualidade dos materiais.

Controlo de Produção

A KIS, Lda. implementará um sistema eficaz de controlo de produção para garantir que todos os processos operacionais sejam eficientes, económicos e em conformidade com os padrões de qualidade definidos. A gestão do controlo de produção será realizada através de um conjunto de processos e sistemas que permitirão monitorizar o fluxo de trabalho, os níveis de estoque e a qualidade dos produtos em todas as fases da produção. Os principais mecanismos de controlo de produção incluem:

1. Gestão de Inventário e Materiais

A gestão de inventário será realizada através de um sistema de software ERP (Enterprise Resource Planning) integrado, que permitirá monitorizar em tempo real o nível de matérias-primas, componentes e produtos acabados. O controlo de inventário será feito com o objetivo de evitar excessos ou faltas de materiais, minimizando assim os custos de armazenamento e evitando a interrupção da produção.

- Níveis de inventário: A KIS, Lda. definirá limites de inventário mínimo e máximo para cada componente essencial. Estes níveis serão revistos periodicamente com base na previsão de demanda.

- Reabastecimento “*Just-in-Time*” (JIT): O sistema de reabastecimento será implementado com base no modelo JIT, o que ajudará a reduzir os custos de armazenamento e garantir que os materiais sejam adquiridos conforme a necessidade de produção.

2. Gestão de Produção e Planificação

A KIS, Lda. utilizará um sistema de planeamento de recursos de produção (MRP - *Material Requirements Planning*) que ajudará a coordenar as atividades de produção com as previsões de demanda, os recursos disponíveis e os prazos de entrega.

O MRP irá garantir que todos os componentes necessários para a produção estejam disponíveis no momento certo, e que a produção seja organizada de forma a maximizar a eficiência e minimizar os tempos de inatividade.

A produção será planeada com base nas previsões de vendas e nas encomendas recebidas, com um sistema flexível que permite ajustar a capacidade produtiva conforme a procura.

O planeamento será realizado trimestralmente, com revisões mensais para ajustar a produção às flutuações do mercado.

O controlo de qualidade será implementado em todas as fases da produção, incluindo a receção de matérias-primas, a montagem dos dispositivos, a calibração e os testes de funcionalidade. Cada etapa será monitorizada e documentada para garantir que todos os produtos atendem aos padrões de qualidade estabelecidos.

3. Mecanismos de Qualidade e Testes

A KIS, Lda. implementará um rigoroso sistema de controlo de qualidade para garantir que todos os dispositivos atendam aos requisitos de desempenho e segurança antes de serem enviados para os clientes. A qualidade será monitorizada através de:

- **Testes de Produção:** Antes da embalagem, cada dispositivo passará por um conjunto de testes de funcionalidade e desempenho, incluindo testes de sensores biométricos (precisão e rapidez de leitura), testes de criptografia e testes de resistência física (durabilidade da carcaça, resistência à água e impacto). Esses testes serão realizados de forma automatizada, através de equipamentos de teste especializados.

- **Inspeção Visual e Funcional:** A cada ciclo de produção, será realizada uma inspeção visual e funcional de amostras aleatórias dos dispositivos, para verificar que não há defeitos estéticos ou funcionais. Isso ajudará a garantir que os produtos finais estejam em conformidade com as especificações técnicas.

- **Certificação de Segurança:** A KIS, Lda. buscará a certificação de segurança internacional para os dispositivos, de forma a garantir que o produto atenda às normas e regulamentos de segurança de diferentes mercados internacionais. Isso incluirá a obtenção de certificações de conformidade com os padrões de segurança de dados e a proteção contra riscos digitais.

4. Monitorização de Produção e Indicadores de Performance

Para assegurar a eficiência e o cumprimento dos objetivos de produção, a KIS, Lda. implementará uma série de indicadores-chave de performance (KPIs) que serão monitorizados ao longo de todo o processo de produção. Alguns exemplos desses indicadores poderão ser:

- Taxa de Defeitos: Percentual de unidades produzidas que não atendem aos padrões de qualidade.
- Taxa de Cumprimento de Prazo: Percentual de encomendas entregues dentro do prazo estipulado.
- Custo por Unidade Produzida: O custo médio de produção por unidade, que será monitorizado para garantir que a produção se mantenha dentro do orçamento e que os custos sejam otimizados ao longo do tempo.
- Eficiência de Produção: Medição da relação entre a produção real e a produção prevista, com o objetivo de maximizar a capacidade produtiva sem comprometer a qualidade.

5. Relacionamento com Fornecedores e Gestão de Pedidos

O controlo de produção também incluirá uma gestão eficiente da cadeia de fornecimento. A KIS, Lda. estabelecerá relações de longo prazo com os fornecedores, o que permitirá negociar melhores condições de fornecimento, manter uma comunicação constante para garantir a entrega atempada dos componentes e garantir que os materiais adquiridos atendam às normas de qualidade estabelecidas.

Para cada pedido de componentes, será realizado um controlo detalhado das datas de entrega, de forma a garantir que todos os componentes necessários para a produção sejam entregues de acordo com o planeamento. O sistema ERP alertará para qualquer desvio ou atraso nas entregas.

Serão definidos acordos de nível de serviço (“Service Level Agreement” ou “SLA”) com cada fornecedor para garantir que os materiais sejam entregues dentro dos prazos estabelecidos, com o mínimo de variações possíveis. Isso permitirá que a KIS, Lda. mantenha a continuidade da produção sem interrupções.

Considerações Ambientais e Sustentabilidade:

O KIS será projetado com foco na matéria de sustentabilidade. A bateria recarregável e a utilização de materiais recicláveis, como o alumínio e TPU, garantem que o produto minimize o impacto ambiental. Além disso, será implementado um plano de reciclagem para o dispositivo quando chegar ao fim de sua vida útil, de forma a proporcionar uma solução responsável para a gestão de resíduos eletrônicos.

O processo de desenvolvimento e produção será orientado por práticas sustentáveis, com foco na redução de desperdícios e na utilização de materiais ecológicos sempre que possível.

ESTRATÉGIA COMERCIAL

A estratégia comercial da KIS, Lda. visa posicionar o nosso produto de forma competitiva no mercado, ao destacar os benefícios específicos de segurança e inovação que ele oferece. Nesse contexto, apresenta-se um plano detalhado com exemplos e valores meramente especulativos para a realização do exercício da estratégia comercial:

Definição de Preço

A definição do preço é essencial para garantir a atratividade do produto e a sua competitividade no mercado.

Custos de Produção:

- **Matérias-primas:** O dispositivo KIS incluirá componentes como sensores biométricos (custo unitário de 20€), processadores de alta performance (custo unitário de 30€), módulos de armazenamento seguro (custo unitário de 10€) e outras partes eletrônicas, com um custo médio de 80€ por unidade.

- **Mão de obra:** A produção manual e a montagem de cada dispositivo têm um custo estimado de 15€ por unidade.

- **Logística e distribuição:** O custo de embalagem e envio por unidade é estimado em 5€, considerando um modelo de distribuição nacional.

Custo total de produção por unidade: 80€ (componentes) + 15€ (mão de obra) + 5€ (distribuição) = 100€ por unidade.

Custos de Marketing e Distribuição:

- Publicidade digital (Google Ads, Facebook Ads): Um orçamento inicial de 3.000€ para campanhas de marketing digital, com um custo médio de 1€ por clique. Espera-se um total de 3.000 cliques por mês, com uma taxa de conversão de 2%, o que resulta em 60 vendas mensais.
- Promoções e Feiras: Participação em feiras de tecnologia, com um custo anual de 5.000€, cobrindo o aluguer de estandes e materiais promocionais.

Preço Final de Venda:

- Cálculo do Preço Base: O preço relativamente aos custos de produção e marketing será de 100€ (custo de produção) + 40€ (margem de marketing e distribuição) = 140€.
- Preço de Venda ao Público: A KIS, Lda. determinará o preço final de venda com base em uma margem de lucro de 100% sobre o custo total de produção, o que traduz um preço final de 280€ por unidade.

Identificação do Público-Alvo e Segmentação

A KIS, Lda. direcionará a sua oferta a diferentes segmentos de clientes, conforme detalhado abaixo:

Segmentos:

- Empresas: Focadas em melhorar a segurança digital, como bancos e empresas de tecnologia, que necessitam de sistemas de autenticação eficazes.
- Consumidores individuais: Profissionais e pessoas preocupados com a segurança digital e proteção de dados (ex. profissionais de TI, executivos, pessoas com criptoativos).
- Para empresas de médio porte, a KIS, Lda. irá identificar clientes com entre 50 e 500 funcionários, localizados em grandes cidades como Lisboa, Porto e Faro. Estima-se que 20% dessas empresas necessitam de uma solução de segurança biométrica, o que representa um mercado de 2.000 empresas.

- Para consumidores individuais, será feita uma segmentação baseada na idade (25-45 anos), com rendimentos anuais superiores a 30.000€, localizados em áreas urbanas.

3. Canais de Vendas

A estratégia de vendas da KIS, Lda. será indireta, apresentada através do site institucional que apenas indicará os locais autorizados de venda e respetivos marketplaces:

Canais Indiretos:

- Distribuidores: A KIS, Lda. irá estabelecer parcerias com distribuidores especializados em equipamentos de segurança digital e tecnologia de ponta. Estima-se uma margem de comissão de 10% sobre cada venda realizada por distribuidores.

- Revendedores e Parceiros: Através de alianças com empresas de tecnologia e segurança que já atuam em mercados adjacentes (como empresas de software de criptografia), que podem distribuir o produto como parte de um pacote de soluções.

Comunicação e Imagem da Marca

A imagem da KIS será projetada para transmitir inovação, confiança e especialização em segurança digital.

- Campanhas Digitais: Utilização de anúncios pagos no Google Ads e redes sociais como LinkedIn e Facebook, com um orçamento mensal de 3.000€. Serão produzidos anúncios visuais e vídeos demonstrando as funcionalidades do produto, com foco na segurança biométrica e na proteção de criptoativos.

- Participação em Feiras: A KIS, Lda. participará em eventos de tecnologia e segurança (ex. Web Summit), com custo estimado de 5.000€ por evento (aluguer de estande e materiais promocionais).

- Testemunhos e Casos de Sucesso: A KIS, Lda. irá criar um site de testemunhos e casos de sucesso, incluindo entrevistas com clientes satisfeitos e parceiros, que irão reforçar a confiança na marca.

Ações de Marketing

As ações de marketing serão ajustadas para garantir uma alta taxa de conversão e maximizar o impacto do lançamento do produto.

- Lançamento de Produto: Promoções de lançamento com desconto de 10% nas primeiras 100 unidades vendidas. Exemplo: preço inicial de 280€, com desconto de 10%, resultando em um preço de 252€ nas primeiras vendas.
- Promoção para Empresas: Oferta de pacotes especiais para empresas, com desconto de 15% em compras de mais de 10 unidades.
- Marketing de Conteúdo: Criação de artigos de blog e vídeos explicativos sobre segurança digital e como o dispositivo KIS pode ajudar na proteção de dados sensíveis e criptoativos.

Monitorização e Avaliação de Resultados

A KIS, Lda. monitorará continuamente os resultados da estratégia comercial através de KPIs como:

- Taxa de Conversão: A taxa de conversão de visitantes em compradores será monitorada através do Google Analytics, com objetivo de atingir uma taxa de conversão mínima de 3%.
- Custo de Aquisição de Cliente (CAC): O CAC será calculado com base no custo total de marketing e vendas dividido pelo número de clientes adquiridos. O objetivo será manter o CAC abaixo de 150€ por cliente.
- ROI de Marketing: O ROI de cada campanha será avaliado com base na receita gerada, com objetivo de alcançar uma rentabilidade de pelo menos 200% sobre o investimento.

GESTÃO E CONTROLO DO NEGÓCIO

A KIS, Lda. compromete-se a garantir um controlo rigoroso e transparente de todos os processos empresariais desde o início da operação. O objetivo é não apenas cumprir com as obrigações legais, mas também otimizar a gestão e o crescimento sustentável da empresa. Este controlo será realizado com base em relatórios regulares e indicadores chave de desempenho (KPIs) nas três áreas fundamentais: Vendas, Produção e Controlo Financeiro. Nesse contexto, apresenta-se um plano detalhado com exemplos e valores meramente especulativos para a realização do exercício da gestão e controlo do negócio:

1. Relatórios Regulares

A KIS, Lda. produzirá relatórios mensais e trimestrais que serão utilizados para monitorizar o progresso do negócio, identificar desvios e implementar ações corretivas. Estes relatórios serão dirigidos à gestão interna e disponibilizados aos auditores, fiscais e instituições bancárias quando necessário.

2. Áreas de Controlo

Vendas: O controlo das vendas será realizado utilizando um sistema de CRM (Customer Relationship Management), como por exemplo o Zoho CRM, com um custo médio de 12€ por utilizador/mês para pequenas empresas. Este sistema permitirá recolher dados detalhados sobre as vendas, como:

- Vendas por tipo de produto: Relatório mensal que apresenta a distribuição percentual das vendas por tipo de produto, como, por exemplo, 70% atribuídos ao dispositivo KIS.
- Vendas por cliente: Monitorização das vendas realizadas a clientes específicos, permitindo uma análise de dependência de clientes. Exemplo: 30% das vendas provenientes de 5 clientes principais.
- Vendas por vendedor: Relatórios sobre o desempenho individual da equipa de vendas, permitindo identificar melhores práticas e áreas de melhoria.
- Vendas originadas por visitas e chamadas: Relatório sobre as vendas resultantes de esforços diretos de vendas, como visitas ao cliente ou chamadas telefónicas.

Produção: O controlo da produção será feito com base em software de gestão de produção como o ERP PHC, com custos de licenciamento anuais a partir de 1.500€ por licença, permitindo à empresa monitorizar o processo de produção e controlar os custos. Os indicadores de produção incluirão:

- Custos de produção: Relatórios mensais sobre o custo de materiais e energia utilizados na produção dos dispositivos KIS. Exemplo: O custo de material para fabricar um dispositivo de autenticação biométrica é de 50€, e o custo de energia por unidade produzida é de 2€.

- Tempo de produção: A medição do tempo médio necessário para produzir um dispositivo de autenticação, sendo o objetivo reduzir esse tempo a 5 horas por unidade a partir de 6 horas iniciais.

- Taxa de desperdício: Monitorização da taxa de desperdício de materiais, com o objetivo de reduzir o desperdício de componentes eletrónicos para 3% do total consumido.

- Desempenho das máquinas: Relatório sobre a eficiência das máquinas de produção, como a taxa de utilização das máquinas de soldagem, que deverá atingir 90% da capacidade produtiva.

Além disso, a empresa terá um Sistema de Gestão da Qualidade (SGQ) para monitorizar os padrões de produção e garantir que os dispositivos atendem aos requisitos de qualidade, com auditorias internas realizadas mensalmente.

3. Controlo Financeiro: A KIS, Lda. utilizará um software de contabilidade como o Sage 50cloud, com custos anuais a partir de 400€, para gerir as finanças da empresa. Este sistema permitirá gerar relatórios financeiros detalhados, incluindo:

- Balanço financeiro e Demonstração de resultados: o balanço financeiro, com atualização trimestral sobre ativos, passivos e capital próprio, e a demonstração de resultados, com análise mensal das receitas e despesas, permitindo identificar o lucro líquido e a margem operacional, como no exemplo em que, ao vender um produto por 250€ com custo de produção de 100€, a margem de lucro será de 150€ por unidade.

- Fluxo de caixa: Relatório diário sobre os recebimentos e pagamentos, ajudando a gerir o capital de giro da empresa e evitando a falta de liquidez.

Inicialmente, a função contabilística será realizada por um contabilista interno a tempo parcial, com custos mensais de cerca de 800€. À medida que a empresa crescer, será criada uma equipa interna de contabilidade e um Departamento Financeiro dedicado.

4. Controlo Adicional

Além do controlo das vendas, produção e finanças, serão implementados os seguintes controlos adicionais:

- Controlo de Qualidade: Será adotada uma política de qualidade com base em normas internacionais, como a ISO 9001. O custo inicial de certificação será de aproximadamente 5.000€, mas permitirá melhorar os processos produtivos e a confiança dos clientes.

- Controlo Ambiental: A empresa compromete-se a seguir as melhores práticas ambientais, com um custo inicial de implementação de 2.000€ para a avaliação ambiental e a instalação de sistemas de gestão de resíduos.

5. Sistemas de Informação

A KIS, Lda. usará o SAP Business One, a um custo anual de 5.000€, para integrar dados operacionais, como vendas, produção, inventário e finanças, num único sistema, garantindo uma gestão eficiente.

6. Auditores

A KIS, Lda. contratará auditores externos, como a KPMG ou PwC, para realizar auditorias anuais. O custo estimado de uma auditoria anual será de cerca de 5.000€, dependendo da complexidade do negócio. A auditoria externa garantirá a conformidade fiscal e regulatória e proporcionará uma análise independente da situação financeira da empresa.

INVESTIMENTO NECESSÁRIO

Para garantir o sucesso e a sustentabilidade do lançamento da KIS, Lda., é necessário um investimento inicial significativo que cobrirá as várias fases do processo, desde a aquisição de instalações e equipamentos até a estruturação da operação e contratação da produção. Este investimento será apoiado por um plano de financiamento cuidadosamente estruturado, que combina tanto fontes de capital próprio como financiamento de terceiros, de modo a equilibrar o risco e assegurar a viabilidade do negócio. Nesse contexto, apresenta-se um plano detalhado com exemplos e valores meramente especulativos para a realização do exercício do cálculo do investimento necessário:

1. Necessidade de Capital Inicial

A KIS, Lda. estima um investimento inicial total de €500.000, destinado a cobrir as seguintes áreas:

- **Aquisição de Instalações e Infraestruturas:** O custo estimado para a aquisição de instalações e adaptação ao processo de produção é de €150.000. Este valor inclui a compra de um espaço de 500 m², bem como as obras de adaptação para instalações de produção e escritório. O espaço será alugado inicialmente com uma opção de compra após três anos, se necessário, permitindo à empresa ajustar o seu modelo de financiamento à medida que o negócio se desenvolve.

- **Equipamento de Produção:** A empresa precisará de equipamentos especializados para a produção dos dispositivos de autenticação biométrica e para a gestão de criptoativos.

O custo estimado de aquisição do equipamento será de €200.000.

Isso inclui:

- Máquinas de soldagem e montagem: €100.000
- Equipamento para teste e controlo de qualidade: €50.000
- Sistema de ERP e software de gestão: €50.000

- Despesas de Capital de Giro e Marketing: Para cobrir as despesas iniciais relacionadas com o capital de giro (estoque de matérias-primas, salários iniciais, custos operacionais de início de atividade), será necessário um montante de €100.000. Este valor também cobrirá as campanhas de marketing e o lançamento da marca KIS no mercado. Estima-se que a empresa necessite de €50.000 em publicidade e promoções para posicionar a marca no mercado, incluindo publicidade digital e física, participação em feiras e eventos.

- Despesas Administrativas e Legais: O custo estimado para cumprir as obrigações legais e administrativas (registo de patentes, licenças, assessoria jurídica e contabilidade) será de €50.000.

2. Fontes de Financiamento

Para financiar este investimento inicial, a KIS, Lda. irá recorrer a duas fontes principais de financiamento:

- Capital Próprio dos Promotores: A empresa contará com €150.000 de capital próprio, sendo aportado pelos fundadores. Esta quantia representará 30% do valor total do investimento inicial e será a primeira linha de financiamento. Este montante será utilizado principalmente para cobrir custos iniciais como a aquisição das instalações e a compra dos equipamentos mais essenciais.

- Financiamento de Capital de Risco (Capital Externo): A KIS, Lda. procurará atrair €200.000 de investidores de capital de risco, que poderão adquirir uma participação minoritária na empresa. Este investimento será crucial para garantir o crescimento acelerado da produção e para cobrir os custos de marketing e expansão. A empresa planeja ceder até 20% do seu capital social para estes investidores, de forma a garantir que os mesmos tenham um retorno adequado sobre o seu investimento à medida que a empresa cresce e se expande no mercado.

- Financiamento Bancário ou Empréstimos: A KIS, Lda. também recorrerá a €150.000 em financiamento bancário, a ser obtido através de um empréstimo a 5 anos, com uma taxa de juros estimada de 4%. O financiamento bancário será utilizado principalmente para cobrir os custos com a aquisição de equipamento e as despesas de capital de giro.

3. Investimento

O investimento será realizado de forma faseada, de acordo com o desenvolvimento das necessidades do negócio:

- Fase 1: Aquisição de Instalações e Equipamento Essencial (3 primeiros meses): O investimento de €300.000 será utilizado na compra e adaptação das instalações e na aquisição dos primeiros equipamentos necessários para iniciar a produção. A fase inicial cobrirá também parte das despesas com marketing e a criação da infraestrutura de vendas.

- Fase 2: Expansão da Produção e Marketing (6 meses seguintes): Durante os próximos 6 meses, será necessário investir €150.000 adicionais em expansão da capacidade de produção e reforço das ações de marketing e publicidade.

- Fase 3: Consolidação e Crescimento do Negócio (12 meses seguintes): O montante restante de €50.000 será utilizado para financiar os custos operacionais contínuos, incluindo a contratação de mais pessoal, aumento do stock de matérias-primas, e ampliação da rede de distribuição e vendas.

4. Compromisso dos Promotores

Os promotores, como fundadores da KIS, Lda., comprometem-se a investir pessoalmente €150.000 como garantia do seu compromisso com o projeto. Este capital próprio é considerado um pré-requisito importante para os investidores de capital de risco e instituições bancárias, pois demonstra a seriedade do projeto e o compromisso dos fundadores em garantir o sucesso da empresa.

PROJEÇÕES FINANCEIRAS / MODELO FINANCEIRO

Para a realização do exercício do modelo financeiro, serão apresentados os detalhes com exemplos e valores calculados com base nos dados meramente especulativos dos exemplos anteriores.

Mapa de Custo de Mercadorias Vendidas e Matérias Consumidas

Mapa de CMVMC	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Nº de Unidades Produzidas (unidades)	1 800,00	2 700,00	4 050,00	4 860,00	5 832,00
Custo dos Sensores Biométricos (€)	45 000,00	67 500,00	101 250,00	121 500,00	145 800,00
Custo do Chip de Criptografia (€)	27 000,00	40 500,00	60 750,00	72 900,00	87 480,00
Custo da Carcaça e Componentes (€)	18 000,00	27 000,00	40 500,00	48 600,00	58 320,00
Custo com Montagem (€)	36 000,00	54 000,00	81 000,00	97 200,00	116 640,00
Custo dos Testes de Qualidade e Segurança (€)	9 000,00	13 500,00	20 250,00	24 300,00	29 160,00
Custo da Embalagem (€)	3 600,00	5 400,00	8 100,00	9 720,00	11 664,00
Custo Total (€)	138 600,00	207 900,00	311 850,00	374 220,00	449 064,00

Tabela 2 - Mapa de Custo de Mercadorias Vendidas e Matérias Consumidas

Análise: Durante o período de cinco anos, estima-se a produção de 19.242 unidades do dispositivo, com um custo total acumulado de 1.481.634,00€. O custo médio por unidade situa-se, assim, em aproximadamente 77,00€. A análise detalhada dos componentes revela uma estrutura de custos dominada por dois elementos críticos: os sensores biométricos, que representam 33% do total (495.050,00€), e os chips de criptografia, com 19,5% (288.630,00€). Estes dois componentes são essenciais para a funcionalidade de segurança e autenticação do dispositivo, que justificam a sua expressão financeira relevante. Outros custos relevantes incluem a montagem (384.840,00€), carcaça e componentes físicos (192.420,00€), testes de qualidade e segurança (96.210,00€) e embalagem (38.484,00€).

O crescimento progressivo dos custos ao longo dos anos acompanha o aumento da produção, mantendo, contudo, uma estrutura de custos proporcional, o que evidencia uma consistência no processo de fabrico.

A evolução previsível dos custos sugere que, apesar do aumento da escala produtiva, não se verificam reduções significativas nos custos unitários ao longo do tempo.

Tal facto indica um plano preventivo e a ausência de economias de escala relevantes, o que poderá justificar a eventual futura necessidade de explorar estratégias de negociação com fornecedores, automação de processos e otimização logística como formas de mitigar o impacto direto no custo unitário e, por consequência, na margem de lucro operacional.

Conclusão: A estrutura de custos apresentada é coerente com a complexidade tecnológica do produto. A gestão eficaz destes custos, especialmente dos mais onerosos, será determinante para a sustentabilidade financeira da empresa. A manutenção da qualidade e segurança do produto deve ser equilibrada com a racionalização de custos operacionais, garantindo competitividade no mercado e atratividade para investidores e parceiros estratégicos.

Fornecimento e Serviços Externos

Serviço	Custo (€)
Publicidade digital	3.000
Promoções e feiras	5.000
Manutenção de software	10.000
Serviços jurídicos	8.000
Consultoria e auditoria	6.000
Total	32.000

Tabela 3 - Fornecimento e Serviços Externos

Análise: O custo anual com fornecimentos e serviços externos representa um investimento necessário para a promoção da marca, conformidade legal e manutenção tecnológica. Recomenda-se a revisão periódica desses custos para otimizar despesas e manter eficiência operacional.

Custos com o Pessoal

Cargo	Salário Mensal (€)	Salário Anual (€)
Sócio Gerente	3.500	42.000
Especialista em Software	3.000	36.000
Especialista Jurídico	2.800	33.600
Especialista em Design de Produto	2.500	30.000
Contabilista	2.000	24.000
Total	-	165.600

Tabela 4 - Custos com o Pessoal

Análise: A estrutura salarial é condizente com a especialização requerida para cada função. O impacto da folha de pagamentos no orçamento operacional requer avaliação constante para garantir competitividade salarial e sustentabilidade financeira.

Investimentos

Item	Custo (€)
Máquinas de soldagem automática	50.000
Máquinas de calibração e teste	40.000
Máquinas de embalagem automatizada	20.000
Computadores e software	15.000
Mobiliário de escritório	5.000
Constituição da sociedade	360
Total	130.360

Tabela 5 - Investimentos

Análise: O investimento inicial foca-se na aquisição de equipamentos de produção e calibração, de forma a garantir eficiência e qualidade no processo produtivo. O montante inicial reflete a necessidade de capital intensivo para infraestrutura tecnológica e operacional.

Arrendamento de Espaço

Item	Custo Mensal (€)	Custo Anual (€)
Espaço alugado	1.600	19.200

Tabela 6 - Arrendamento do Espaço

Análise: Optar pelo aluguer em vez da aquisição reduz a carga inicial de investimento, conferindo flexibilidade financeira para futuras expansões. O custo anual de 19.200€ representa um compromisso significativo, devendo ser avaliado à luz da viabilidade do negócio.

Quadro de Financiamento - Santander (5 anos)

As condições do financiamento são as seguintes:

- Montante solicitado: €200.000
- TAN: EURIBOR a 12 meses (2.584%) + Spread (3.75%) = 6.334%
- TAE: 9.665%
- Prazo: 5 anos
- Juros: Calculados diariamente e vencidos no final do mês
- Comissão de imobilização: 2% sobre o montante inicial
- Comissão de gestão: 0.1% mensal sobre o saldo em dívida
- Comissão de abertura: 0.9% sobre o montante financiado
- Imposto de selo: 4% sobre o montante financiado

Simulação do Financiamento a 5 Anos

Ano	Capital Inicial (€)	Amortização (€)	9,665% Juros (€)	4% IS s/Juros (€)	0,9% Comissão Abertura (€)	1,2% Comissão de Gestão (€)	2% Comissão Imobilização (€)	4% IS s/Comissões (€)	Encargos Totais (€)	Capital final (€)
0	300 000,00	0,00	0,00	0,00	2 700,00	0,00	6 000,00	348,00	9 048,00	300 000,00
1	300 000,00	60 000,00	28 995,00	1 159,80	0,00	3 600,00	0,00	144,00	93 898,80	240 000,00
2	240 000,00	60 000,00	23 196,00	927,84	0,00	2 880,00	0,00	115,20	87 119,04	180 000,00
3	180 000,00	60 000,00	17 397,00	695,88	0,00	2 160,00	0,00	86,40	80 339,28	120 000,00
4	120 000,00	60 000,00	11 598,00	463,92	0,00	1 440,00	0,00	57,60	73 559,52	60 000,00
5	60 000,00	60 000,00	5 799,00	231,96	0,00	720,00	0,00	28,80	66 779,76	0,00
Total	-	300 000,00	86 985,00	3 479,40	2 700,00	10 800,00	6 000,00	780,00	410 744,40	-

Tabela 7 - Simulação do Financiamento a 5 anos

Análise do Financiamento

O financiamento apresenta uma estrutura de amortização linear, onde a empresa reembolsa anualmente um valor fixo de capital (€60.000), enquanto os juros diminuem gradualmente à medida que o capital em dívida é amortizado.

A taxa de juro nominal (TAN de 9,665%) implica encargos significativos no início do financiamento, com juros no primeiro ano de €28.995, reduzindo progressivamente até €5.799 no último ano. Os encargos adicionais representam €20.280, sendo os mais relevantes a comissão de imobilização (€6.000), a comissão de gestão (€10.800) e o imposto de selo sobre juros e comissões (€4.259,40). Estes custos adicionais, cobrados sobretudo nos primeiros anos, aumentam a necessidade de liquidez inicial e afetam a estrutura de custos fixos da empresa.

O custo total do financiamento (€410.744,40) representa um acréscimo de 36,9% face ao montante inicialmente financiado (€300.000), refletindo o impacto acumulado dos juros e encargos bancários ao longo do período.

Para garantir a sustentabilidade do projeto, é essencial que as receitas operacionais cubram, de forma consistente, os encargos financeiros anuais, particularmente nos primeiros exercícios, em que o negócio ainda se encontra em fase de maturação e consolidação.

Conclusão: O financiamento apresenta um peso significativo nos primeiros anos, mas a amortização linear permite uma redução gradual dos juros e uma maior previsibilidade nos fluxos de saída. A empresa deverá assegurar um volume de receitas e margens suficientes para cobrir estes encargos, salvaguardando a sua liquidez e capacidade de investimento ao longo do tempo.

Demonstração de Resultados (5 Anos)

Demonstração de	Ano 0	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Resultados						
Investimento Inicial (€)	500 000,00	-	-	-	-	-
Volume de Negócios (€)	-	516 600,00	787 815,00	1 201 095,00	1 464 561,00	1 785 369,60
CMVMC (€)	-	138 600,00	207 900,00	311 850,00	374 220,00	449 064,00
Outsourcing (€)	-	60 000,00	10 000,00	150 000,00	200 000,00	250 000,00
Margem Bruta (€)	-	318 000,00	569 915,00	739 245,00	890 341,00	1 086 305,60
FSE (€)	-	32 000,00	32 000,00	32 000,00	32 000,00	32 000,00
Gastos com Pessoal (€)	-	165 600,00	165 600,00	165 600,00	165 600,00	165 600,00
EBITDA (€)	-	120 400,00	372 315,00	541 645,00	692 741,00	888 705,60
Depreciações e Amortizações (€)	-	20 000,00	20 000,00	20 000,00	20 000,00	20 000,00
EBIT (€)	-	100 400,00	352 315,00	521 645,00	672 741,00	868 705,60
Encargos Financeiros (€)	-	93 898,80	87 119,04	80 339,28	73 559,52	66 779,76
Resultado Antes de Impostos (€)	-	6 501,20	265 195,96	441 305,72	599 181,48	801 925,84
IRC - 21% (€)	-	1 365,25	55 691,15	92 674,20	125 828,11	168 404,43
Resultado Líquido (€)	-500 000,00	5 135,95	209 504,81	348 631,52	473 353,37	633 521,41

Tabela 8 - Demonstração de Resultados (5 Anos)

Análise e Interpretação da Demonstração de Resultados

1. Crescimento do Volume de Negócios

O volume de negócios regista um crescimento significativo ao longo dos cinco anos, iniciando-se com 516.600€ no Ano 1 e alcançando 1.785.369,60€ no Ano 5, o que reflete uma estratégia bem-sucedida de penetração de mercado, combinada com um modelo de crescimento em duas fases: 50% nos primeiros anos e 20% nos anos seguintes.

2. Custos das Mercadorias Vendidas e Matérias Consumidas (CMVMC) e Outsourcing

O CMVMC acompanha o aumento das unidades vendidas, passando de 138.600€ no Ano 1 para 449.064€ no Ano 5.

Os custos com produção externa (“*outsourcing*”) revelam uma gestão progressiva da operação, com uma queda pontual no Ano 2 e um aumento contínuo até atingir 250.000€ no Ano 5, o que reflete uma maior externalização de serviços e possível expansão operacional.

3. Margem Bruta

A margem bruta cresce de forma acentuada, começando em 318.000€ no Ano 1 e atingindo 1.086.305,60€ no Ano 5, o que revela uma estrutura de custos controlada e um forte poder de geração de valor através das vendas. A melhoria contínua da margem bruta comprova a viabilidade do modelo de negócio.

4. Rentabilidade Operacional (EBITDA e EBIT)

O EBITDA é positivo desde o primeiro ano (120.400€), o que demonstra que, desde cedo, a operação consegue gerar resultados antes das amortizações e encargos financeiros.

O EBIT segue a mesma trajetória, com crescimento sólido, atingindo 868.705,60€ no Ano 5, indicando elevada eficiência operacional.

A estabilidade dos gastos com pessoal (165.600€/ano) e das FSE (32.000€/ano) ajuda a consolidar essa performance.

5. Encargos Financeiros

Os encargos financeiros partem de 93.898,80€ no Ano 1 e decrescem até 66.779,76€ no Ano 5, o que representa um alívio progressivo da pressão financeira sobre os resultados. Mesmo nos primeiros anos, os resultados operacionais conseguem cobrir os encargos financeiros, o que demonstra eficácia na estrutura de financiamento.

6. Resultado Antes de Impostos e Lucro Líquido

A empresa apresenta resultados positivos antes de impostos a partir do Ano 1, com um valor inicial de 6.501,20€, que sobe para 801.925,84€ no Ano 5.

Após imposto (IRC 21%), o lucro líquido cresce de forma significativa:

- Ano 1: 5.135,95€
- Ano 3: 348.631,52€
- Ano 5: 633.521,41€

Estes resultados indicam que o projeto alcança o ponto de equilíbrio já no primeiro ano, e evolui rapidamente para níveis de elevada rentabilidade.

7. Investimento Inicial

O investimento inicial de 500.000€ no Ano 0 é compensado ao longo do período de análise com geração acumulada de resultados líquidos superiores ao capital investido, o que indica um período de retorno inferior a 4 anos.

8. Conclusão

A Demonstração de Resultados evidencia um projeto caracterizado por um forte crescimento de receitas, estrutura de custos bem controlada, rentabilidade operacional consistente, redução gradual da dependência de financiamento externo e lucro líquido crescente e sustentável

.A empresa demonstra uma elevada viabilidade económica e financeira, com potencial de expansão e capacidade de reinvestimento e um projeto financeiramente sólido desde o primeiro ano de operação.

9. Cash-Flow de Exploração (5 Anos)

Cash-Flow de Exploração	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
EBIT(1-T) (€)	79	278	412	531	686
	316,00	328,85	099,55	465,39	277,42
Depreciações e Amortizações (€)	20	20 000,00	20 000,00	20 000,00	20 000,00
	000,00				
CF de Exploração (€)	99	298	432	551	706
	316,00	328,85	099,55	465,39	277,42

Tabela 9 - Cash-Flow de Exploração (5 Anos)

Análise do Cash-Flow de Exploração

O Cash-Flow de Exploração (CFE) evidencia a capacidade da empresa em gerar liquidez a partir da sua atividade operacional, antes de considerar investimentos e financiamento.

1. Evolução do CFE

A empresa apresenta desde o primeiro ano um cash-flow de exploração positivo, no valor de 99.316€, o que reflete a capacidade de gerar resultados operacionais após impostos mesmo numa fase inicial do projeto.

2. Contributo do EBIT e Depreciações

O CFE resulta da soma do EBIT após impostos ($EBIT \times (1-Taxa)$) e das depreciações e amortizações, que representam um custo não monetário, sendo reintroduzido no cálculo do fluxo de caixa.

- A estabilidade das depreciações em 20.000€/ano contribui para um reforço constante do cash-flow disponível.
- O crescimento do EBIT(1-T) revela uma melhoria contínua da eficiência operacional e controlo de custos, com destaque para a subida de 79.316€ no Ano 1 para 686.277,42€ no Ano 5.

3. Capacidade de Geração de Liquidez

A progressão do CFE demonstra que a empresa possui uma estrutura de exploração sólida, com crescente capacidade de gerar recursos internos para:

- Cobrir as suas necessidades de fundo de maneiio;
- Amortizar dívidas;
- Reinvestir no crescimento;
- Remunerar os investidores.

Conclusão

A empresa apresenta um perfil financeiro eficaz, ao gerar cash-flows operacionais positivos e crescentes desde o primeiro ano. Este desempenho confirma a viabilidade económica do projeto e a sustentabilidade da operação, ao assegurar a sua capacidade de autofinanciamento e ao reduzir a dependência de capital externo ao longo do tempo.

Necessidades de Fundo de Maneio (NFM)

Necessidades de Fundo de Maneio	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Volume de Negócios (€)	516 600,00	787 815,00	1 201 095,00	1 464 561,00	1 785 369,60
% do VN	3%	3%	4%	4%	4%
Fundo de Maneio (€)	15 498,00	23 634,45	48 043,80	58 582,44	71 414,78
NFM (€)	15 498,00	8 136,45	24 409,35	10 538,64	12 832,34

Tabela 10 - Necessidades de Fundo de Maneio (NFM)

Análise das Necessidades de Fundo de Maneio

As Necessidades de Fundo de Maneio (NFM) acompanham a evolução do volume de negócios e refletem os recursos financeiros requeridos para assegurar o normal funcionamento das operações da empresa, designadamente ao nível do ciclo operacional (stocks, clientes e fornecedores).

No primeiro ano, a NFM é de €15.498, representando 3% do volume de negócios. No segundo ano, apesar do aumento do volume de vendas, observa-se uma redução da necessidade líquida (€8.136), justificada pela maior eficiência na gestão operacional e possível diluição de custos fixos. A partir do terceiro ano, a percentagem aplicada ao volume de negócios aumenta para 4%, o que gera um crescimento mais expressivo das necessidades, ao atingir €24.409, €10.538 e €12.832 nos anos seguintes.

Esta trajetória revela um controlo eficaz nas necessidades de financiamento de curto prazo, com flutuações compatíveis com a evolução do negócio e com o esforço de otimização do ciclo de caixa. A moderação do crescimento da NFM é um sinal positivo para a estabilidade financeira da empresa, o que irá garantir uma margem operacional suficiente para suportar a expansão.

Conclusão: A empresa mantém uma estrutura de fundo de maneo ajustada ao crescimento projetado, ao evidenciar uma gestão prudente dos recursos circulantes. O aumento gradual da NFM é sustentado por uma maior escala de operações e permanece em níveis controláveis, o que contribui para a eficácia financeira do negócio.

10. Valor Residual (5º Ano)

Valor Residual	N
CF exploração último ano (€)	706 277,42
NFM (€)	12 832,34
Tx. de crescimento (g)	2%
(CF-NFM)*(1+g) (€)	707313,9816
Capital Próprio (€)	150000,00
Capital Alheio (€)	350000,00
Tx Ativo Isento de Risco	3,29%
Beta	1,27
Prémio de Risco de Mercado	5,93%
Rentabilidade dos Capitais Próprios	10,82%
WACC	9%
Valor Residual (€)	10.731.390,28

Tabela 11 - Valor Residual (5º Ano)

Análise do Valor Residual

O Valor Residual, estimado em 10 731 390,28 €, traduz a projeção do valor económico da empresa a partir do final do quinto ano, ao assumir a continuidade operacional.

- **Criação de Valor Sustentado**

O elevado valor demonstra que o projeto gera cash-flows eficazes e duradouros, que justificam a atribuição de um valor de mercado elevado no final do horizonte analítico.

- **Equilíbrio Financiamento vs. Rentabilidade**

A rentabilidade dos capitais próprios (10,82%) excede o custo de capital (9%), o que confirma que o negócio remunera de forma superior o risco assumido pelos acionistas. Esta diferença positiva (spread de 1,82 p.p.) contribui de modo decisivo para o valor residual.

- **Sensibilidade ao Crescimento e WACC**

Pequenas variações na taxa de crescimento (g) ou no WACC têm impacto direto no valor residual. Um aumento de g ou redução do WACC reforçaria ainda mais o valor calculado, enquanto o inverso poderia diminuí-lo significativamente.

Conclusão: O valor residual estimado em 10,7 M€ é indicativo de um negócio financeiramente sólido, com capacidade de geração de cash-flows perpétuos e de alto valor para os acionistas. A combinação de um crescimento estável, um WACC competitivo e cash-flows operacionais elevados torna este projeto particularmente atrativo num horizonte de longo prazo.

11. Cash-Flow de Investimento (5 Anos)

Cash-Flow de Investimento	Ano 0	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
CAPEX (€)	500 000,00					
NFM (€)		15 498,00	8 136,45	24 409,35	10 538,64	12 832,34
Valor Residual (€)						10 731 390,28
CF de Investimento (€)	500 000,00	15 498,00	8 136,45	24 409,35	10 538,64	-10 718 557,93

Tabela 12 - Cash-Flow de Investimento (5 Anos)

Análise do Cash-Flow de Investimento

O Cash-Flow de Investimento (CFI) reflete os movimentos financeiros associados à aquisição de ativos fixos, variações nas necessidades de fundo de manuseio (NFM) e à realização do valor residual no final do projeto.

1. Investimento Inicial

No Ano 0, a empresa realiza um investimento de 500.000€, correspondente à aquisição de ativos imobilizados essenciais ao arranque da operação. Este valor representa o compromisso inicial de capital e constitui o maior gasto de investimento até ao último ano.

2. Acompanhamento da NFM

Durante os Anos 1 a 4, o Cash-Flow de Investimento é impactado por incrementos progressivos das Necessidades de Fundo de Maneio (NFM), que representam capital adicional imobilizado para sustentar o crescimento da atividade. Estes valores são tratados como saídas de caixa no âmbito do investimento e refletem a necessidade de capital circulante adicional a cada período.

3. Valor Residual

No Ano 5, considera-se a realização de um valor residual de 10.731.390,28€ e estima-se o valor de mercado do negócio ou dos ativos acumulados. Este montante é registado como uma entrada de caixa significativa, de forma a compensar os investimentos anteriores.

O efeito líquido no Ano 5 resulta num cash-flow de investimento positivo de 10.718.557,93€, depois de descontadas as NFM desse ano.

Conclusão

O Cash-Flow de Investimento é marcado por um grande esforço de capital no início do projeto, seguido por ajustes anuais moderados relacionados com as necessidades operacionais crescentes. No quinto ano, a recuperação do valor residual proporciona uma reversão acentuada, com impacto muito positivo na estrutura financeira do projeto.

Esta trajetória reflete um modelo de investimento concentrado no arranque e valorização ao longo do tempo, adequado a projetos de base tecnológica e inovação.

A forte geração de valor no final do ciclo comprova a atratividade e rentabilidade do investimento.

12. Cash-Flow Global (5 Anos)

Cash-Flow Global	Ano 0	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
CF de Exploração (€)		99 316,00	298 328,85	432 099,55	551 465,39	706 277,42
CF de Investimento (€)	500 000,00	15 498,00	8 136,45	24 409,35	10 538,64	-10 718 557,93
CF Global (€)	-500 000,00	83 818,00	290 192,40	407 690,20	540 926,75	11 424 835,36

Tabela 13 - Cash-Flow Global (5 Anos)

Análise do Cash-Flow Global

O Cash-Flow Global (CFG) representa a evolução líquida da tesouraria do projeto, combinando os fluxos operacionais (CF de Exploração) e os fluxos de investimento (CF de Investimento).

1. Ano 0 – Investimento Inicial

No Ano 0, o projeto regista um gasto único de 500.000€, correspondente ao investimento inicial. Este valor é negativo e reflete a saída de capital necessária para o arranque da atividade. Não há resultados de caixa neste ano.

2. Anos 1 a 4 – Geração Progressiva de Caixa

Nestes anos, o projeto atinge equilíbrio financeiro e demonstra capacidade de autofinanciamento, com fluxos líquidos positivos em todos os períodos. O impacto do investimento residual (NFM) é absorvido pela eficácia da geração de caixa operacional.

3. Ano 5 – Realização do Valor Residual

No Ano 5, o projeto regista um salto significativo no CF Global, atingindo 11.424.835,36€, resultado da conjugação do cash-flow de exploração (706.277,42€) com a entrada líquida do valor residual de 10.731.390,28€, após deduzida a NFM do ano.

Conclusão

O Cash-Flow Global apresenta:

- Fase inicial com saída de capital significativa (Ano 0);
- Geração operacional progressiva e sustentável entre os Anos 1 e 4, com saldos líquidos positivos crescentes;
- Valorização expressiva no Ano 5, com retorno exponencial motivado pela alienação ou valorização do negócio.

Este comportamento confirma a viabilidade financeira do projeto e a sua capacidade de criar valor no médio e longo prazo, sendo particularmente atrativo do ponto de vista do investidor.

Conclusão Final

A análise dos cash-flows evidencia que o projeto segue um ciclo financeiro estruturado e sustentável:

1. **Fase inicial (Ano 0):** Exige um investimento inicial elevado de 500.000€, essencial para a aquisição de ativos e estruturação do negócio.
2. **Fase de arranque e crescimento (Anos 1 e 2):** O negócio começa a gerar cash-flows operacionais positivos desde o primeiro ano, com uma evolução significativa no segundo ano, o que demonstra uma boa capacidade de conversão operacional e controlo dos custos fixos.

3. **Fase de expansão e consolidação (Anos 3 e 4):** Verifica-se uma forte aceleração na geração de caixa, com aumento sustentado da rentabilidade operacional e um impacto marginal dos investimentos adicionais (NFM), o que reflete uma maior eficiência financeira.
4. **Fase de maturação e valorização (Ano 5):** O projeto atinge o seu ponto mais elevado com um cash-flow global de mais de 11 milhões de euros, que será impulsionado pelo valor residual estimado do negócio (10,7M€), que reflete que o seu potencial de mercado e atratividade para eventuais alienações ou novos ciclos de investimento.

Em suma, o projeto revela-se financeiramente viável e atrativo, com retornos crescentes e sustentáveis a médio prazo. A sustentabilidade do cash-flow de exploração, o controlo do investimento incremental e a valorização expressiva no final do ciclo evidenciam um modelo de negócio bem estruturado, com capacidade de gerar valor e retorno sobre o investimento inicial de forma clara e eficaz.

Mapa de Vendas (5 Anos)

Mapa de Vendas	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Preço (€)	280,00	280,00	280,00	280,00	280,00
Nº Unidades Vendidas	1 800,00	2 700,00	4 050,00	4 860,00	5 832,00
Vendas (€)	504 000,00	756 000,00	1 134 000,00	1 360 800,00	1 632 960,00
IVA- 23% (€)	115 920,00	173 880,00	260 820,00	312 984,00	375 580,80
Vendas c/IVA (€)	619 920,00	929 880,00	1 394 820,00	1 673 784,00	2 008 540,80
Prazo Médio de Recebimentos (dias)	60,00	55,00	50,00	45,00	40,00
Saldo de Clientes (€)	103 320,00	142 065,00	193 725,00	209 223,00	223 171,20
Recebimentos (€)	516 600,00	787 815,00	1 201 095,00	1 464 561,00	1 785 369,60

Tabela 14 - Mapa de Vendas (5 Anos)

Análise do Mapa de Vendas

O Mapa de Vendas reflete uma trajetória de crescimento sustentado, com um modelo de crescimento de duas etapas: crescimento acentuado de 50% nos anos 2 e 3, seguido de um crescimento mais moderado de 20% nos anos 4 e 5. Ao longo dos 5 anos, estima-se a venda de 19.242 unidades, o que corresponde a um volume de vendas acumulado de 5.387.760,00€ (sem IVA). O preço unitário mantém-se constante nos 280,00€, o que permite uma comparação clara da evolução em termos de volume. Este fator indica uma política de preços estável, compatível com uma estratégia de penetração de mercado e consolidação da marca.

Os recebimentos anuais acompanham o crescimento das vendas, que atingem 1.785.369,60€ no quinto ano, o que representa mais do triplo do valor recebido no primeiro ano (516.600,00€). Esta evolução tem impacto direto na tesouraria da empresa e evidencia a necessidade de um sistema eficaz de gestão de cobranças.

O prazo médio de recebimentos irá reduzir de 60 para 40 dias, o que constitui um fator positivo em termos de liquidez, uma vez que irá reduzir o ciclo de conversão de caixa. Apesar disso, o saldo de clientes aumenta de 103.320,00€ para 223.171,20€, o que reflete um maior volume de negócios realizados a crédito. Este crescimento exige um controlo rigoroso do risco de crédito e uma política ativa de gestão de contas a receber.

O IVA representa 23% do total das vendas, que se traduz num valor significativo ao longo do período (cerca de 1.239.184,80€). Esta componente tem implicações fiscais relevantes, que exigem um planeamento financeiro cuidadoso para assegurar o cumprimento das obrigações fiscais sem comprometer a liquidez.

Conclusão: A empresa projeta um crescimento consistente e sustentável das vendas, com uma melhoria progressiva na gestão de recebimentos. A estabilidade do preço por unidade e a redução dos prazos médios de recebimento fortalecem a posição de tesouraria. No entanto, o aumento do saldo de clientes e o peso do IVA nas transações irão exigir mecanismos de controlo financeiro eficazes para garantir a eficácia operacional e fiscal da empresa.

Plano Financeiro (5 Anos)

Ano	1° Ano (€)	2° Ano (€)	3° Ano (€)	4° Ano (€)	5° Ano (€)
Receita Bruta (€)	318.000	569.915	739.245	890.341	1.086.305,60
Outsourcing (€)	(60.000)	(100.000)	(150.000)	(200.000)	(250.000)
Custos Fixos (€)	(120.400)	(120.400)	(120.400)	(120.400)	(120.400)
Custos Variáveis (€)	(138.600)	(207.900)	(311.850)	(374.220)	(449.064)
Lucro Bruto (€)	120.400	372 315,00	541 645,00	692 741,00	888 705,60
Encargos Financeiros (€)	93 898,80	87 119,04	80 339,28	73 559,52	66 779,76
Impostos (IRC) (€)	1 365,25	55 691,15	92 674,20	125 828,11	168 404,43
Lucro Líquido (€)	5 135,95	209 504,81	348 631,52	473 353,37	633 521,41

Tabela 15 - Plano Financeiro (5 Anos)

Análise do Plano Financeiro

O Plano Financeiro apresenta um crescimento sustentável da receita bruta, que quadruplica ao longo dos cinco anos, impulsionado pela expansão do mercado e adoção do produto.

Os custos fixos aumentam de forma controlada, enquanto os custos variáveis acompanham o crescimento das vendas.

O lucro bruto demonstra uma tendência ascendente, atingindo 910.000€ no quinto ano, evidenciando uma margem operacional elevada. A carga fiscal cresce proporcionalmente ao aumento do lucro bruto, sendo o IRC estimado em 24%.

O lucro líquido aumenta significativamente, passando de 48.000€ no primeiro ano para 728.000€ no quinto ano, refletindo a viabilidade financeira do negócio.

Rentabilidade (5 anos)

Ano	0	1	2	3	4	5
Tx de Atualização (=wacc)	9%	9%	9%	9%	9%	9%
CF Total	-500 000,00	83 818,00	290 192,40	407 690,20	540 926,75	11 424 835,36
CF Total Atualizado	-500 000,00	77 186,82	246 092,16	318 381,54	389 011,04	7 566 225,63
CF Total Atualizado Acumulado	-500 000,00	-422 813,18	-176 721,02	141 660,51	530 671,56	8 096 897,18
Valor Atual Líquido (VAL)	8 096 897,18					
Taxa Interna de Rentabilidade (TIR)	105%					
Prazo de Recuperação do Investimento (PRI)	1 ano e 7 meses	6,660726293				
Índice de Rentabilidade (IR)	17,19					

Tabela 16 - Rentabilidade (5 anos)

Análise de Rentabilidade

O VAL de 8 096 897,18 € resulta da soma dos cash-flows atualizados descontados à taxa de 9%. Um VAL claramente positivo indica que o valor presente dos benefícios financeiros excede em muito o investimento inicial, o que demonstra uma criação de valor valiosa para os acionistas. Relativamente à Eficácia na Geração de Valor o elevado VAL e o IR (muito superior a 1), demonstram que o projeto converte de forma extremamente eficiente o capital investido em cash-flows futuros. Verifica-se também uma rápida recuperação do capital com o Período de Recuperação do Investimento (PRI) inferior a 2 anos o que indica menor exposição do investidor ao risco temporal e reforça a liquidez do investimento. A rentabilidade excepcional do projeto é comprovada por uma Taxa Interna de Rentabilidade (TIR) de 105% revela uma rentabilidade anual composta extremamente alta, que sugere que o projeto remunera largamente o risco assumido. Por fim, observa-se um claro alinhamento com objetivos de investimento ao considerar a combinação de curto prazo de recuperação, elevado VAL e rentabilidade substancial, este investimento alinha-se com perfis de retorno agressivos, que poderá igualmente servir como *benchmark* para alocação de capital em projetos de tecnologia e inovação.

Conclusão: Os indicadores financeiros apresentam uma avaliação extremamente positiva do investimento: o negócio não apenas recupera rapidamente o capital inicial, como também gera valor substancial ao longo do tempo, com rentabilidades muito acima do custo de capital. Trata-se, portanto, de um projeto financeiramente sólido, de elevada atratividade para investidores e com baixo risco de liquidez.

Balanço (5 Anos)

Balanço	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5
Inventários (€)	0	35 389	30 075	73 944	109 254
Clientes (€)	53 320	142 065	193 725	209 223	223 171
Caixa e Equivalentes (€)	5 166	7 878	12 011	14 646	17 854
Total Ativo Corrente (€)	58 486	185 332	235 811	297 813	350 279
Ativos Intangíveis (€)	0	0	300 000	500 000	750 000
Ativos Fixos Tangíveis (€)	500 000	480 000	460 000	440 000	420 000
Total Ativo Não Corrente (€)	500 000	480 000	760 000	940 000	1 170 000
Total Ativo (€)	558 486	665 332	995 811	1 237 813	1 520 279
Estado e Outros Entes Públicos (€)	41 365	55 691	92 674	125 828	168 404
Outros Passivos Financeiros (€)	61 985	0	0	0	0
Total Passivo Corrente (€)	103 350	55 691	92 674	125 828	168 404
Financiamentos Obtidos (€)	300 000	240 000	180 000	120 000	60 000
Total Passivo Não Corrente (€)	300 000	240 000	180 000	120 000	60 000
Total Passivo (€)	403 350	295 691	272 674	245 828	228 404
Capital Social (€)	150 000	150 000	150 000	150 000	150 000
Reservas Legais (€)	0	5 000	15 000	20 000	35 000
Resultados Transitados (€)	0	5 136	209 505	348 632	473 353
Resultado Líquido do Período (€)	5 136	209 505	348 632	473 353	633 521
Capital Próprio (€)	155 136	369 641	723 136	991 985	1 291 875
Capital Próprio + Passivo (€)	558 486	665 332	995 811	1 237 813	1 520 279

Tabela 17 - Balanço (5 Anos)

Análise do Balanço

A estrutura do balanço ao longo dos cinco anos demonstra uma evolução sólida da posição financeira da empresa, que reflete o crescimento sustentado e o reforço do capital próprio.

Ativo Corrente

O ativo corrente cresce de forma progressiva, passando de 58.486€ no Ano 1 para 350.279€ no Ano 5. Este aumento decorre essencialmente:

- Do reforço dos clientes a receber, fruto do crescimento do volume de negócios a crédito.
- Do crescimento dos inventários, que refletem o aumento da atividade operacional e a preparação para responder à maior procura.
- De uma posição de tesouraria crescente, o que indica uma melhoria na liquidez e na gestão eficiente do cash-flow.

Ativo Não Corrente

O ativo não corrente evolui significativamente:

- Os ativos fixos tangíveis sofrem uma depreciação regular, que reduzem de 500.000€ para 420.000€.
- Os ativos intangíveis são introduzidos a partir do Ano 3, num total de 750.000€ no Ano 5, o que indica um investimento em propriedade intelectual, software, marca ou outros ativos estratégicos.

Este crescimento contribui para o aumento do ativo total, que sobe de 558.486€ no Ano 1 para 1.520.279€ no Ano 5.

Passivo

O passivo apresenta uma redução progressiva:

- O passivo não corrente, relativo a financiamentos obtidos, é amortizado anualmente e reduz de 300.000€ para 60.000€ até ao Ano 5.
- O passivo corrente é composto principalmente por responsabilidades fiscais, que acompanham a evolução da rentabilidade. Passa de 103.350€ no Ano 1 para 168.404€ no Ano 5.

A redução do passivo global, de 403.350€ para 228.404€, evidencia a diminuição do grau de alavancagem e uma maior autonomia financeira.

Capital Próprio

O capital próprio regista uma expansão expressiva ao longo do período:

- Atinge 1.291.875€ no Ano 5, impulsionado pelos resultados líquidos acumulados e pela valorização das reservas legais.
- A rentabilidade consistente desde o Ano 2 permitiu a acumulação de lucros, o que reforça a solidez patrimonial da empresa.

Conclusão

O balanço demonstra uma empresa em forte crescimento e consolidação financeira. A redução do passivo, associada ao aumento do capital próprio e dos ativos estratégicos (intangíveis), indica uma melhoria da eficácia económica, da capacidade de autofinanciamento e da valorização do negócio. A estrutura financeira revela uma trajetória positiva, com sustentabilidade a longo prazo e redução da dependência externa.

LOGÓTIPO E MARCA



Figura 4 - Logótipo e Marca

O logótipo criado para a marca KIS – *Keep It Safe* apresenta um design elegante e tecnológico, idealizado para transmitir segurança, inovação e confiança. O símbolo principal combina a imagem estilizada de um cadeado digital com elementos geométricos suaves e futuristas, que remetem à proteção de dados e ativos digitais.

A paleta de cores utiliza tons metálicos escuros com apontamentos luminosos — cor tradicionalmente associada à tecnologia, fiabilidade e cibersegurança. O nome "KIS" surge em tipografia moderna e angular, que reforça a ideia de tecnologia de ponta, enquanto o slogan "*Keep It Safe*" aparece logo abaixo e integrado de forma discreta, o que cria um equilíbrio visual e transmite de imediato o propósito do dispositivo.

O conjunto comunica um produto premium, focado na segurança digital, com um design adaptado tanto a ambientes corporativos como a consumidores exigentes que valorizam proteção e sofisticação.

Desenho do Produto

O KIS foi projetado com dimensões de 80mm x 40mm x 5mm, otimizadas para portabilidade e utilização confortável:



Figura 5 - KIS - Visão Frontal e ecrã ligado

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D AutoCAD



Figura 6 - KIS - Visão Traseira

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D



Figura 7 - KIS – Visão Diagonal Frontal

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D



Figura 8 - KIS - Visão diagonal traseira esquerda

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D



Figura 9 – KIS - Visão diagonal traseira direita

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D



Figura 10 – Embalagem e selo

Nota: Imagem de autoria própria com recurso à ferramenta de modelagem 3D

Anexo I – Guião do Focus Group

Objetivo da Sessão:

Recolher as perceções, recomendações e validação crítica sobre a proposta de valor e o modelo de negócio do dispositivo KIS – Keep It Safe, com base no Business Model Canvas, em conjunto com um grupo de 4 especialistas com distintas experiências académicas e profissionais nas áreas de sistemas de informação, gestão, segurança digital e inovação tecnológica. A metodologia foi organizada em duas sessões distintas, com funções complementares: a primeira exploratória e a segunda avaliativa.

Participantes:

- Professor Doutor José Agostinho
- Professor Doutor Pedro Mendonça
- Professor Doutor Rui Umberto
- Professor Doutor Luís Rodrigues

Moderador: Omar Soares

Local: Online – Plataforma Zoom

Datas:

- 1.ª Sessão: 03/06/2025
- 2.ª Sessão: 06/06/2025

1.ª Sessão – Apresentação Exploratória e Preparatória

Objetivo da Sessão:

Apresentar em detalhe a proposta do dispositivo KIS e o modelo de negócio base, recolher impressões iniciais dos especialistas e identificar tópicos estratégicos a aprofundar numa segunda sessão estruturada de debate.

Duração Aproximada: 1h

Conteúdo Apresentado:

Apresentação detalhada do dispositivo KIS:

- Funcionalidades (carteira de acessos, armazenamento de criptoativos, backup em cloud, autenticação biométrica)
- Diferenciação face a soluções existentes
- Design e dimensões do produto

Apresentação detalhada do modelo de negócio (Business Model Canvas):

- Proposta de valor
- Segmentos de clientes
- Canais
- Relacionamento com o cliente
- Fontes de receita
- Recursos-chave
- Atividades-chave
- Parceiros-chave
- Estrutura de custos

Metodologia:

- Apresentação com apoio de slides
- Debate livre orientado por observações e perguntas dos participantes
- Registo das sugestões, dúvidas e temas levantados para posterior sistematização

Resultado da Sessão:

Identificação dos temas considerados mais críticos ou estratégicos para debate aprofundado:

- Estratégia multissegmento (B2C vs B2B)
- Confiabilidade dos canais de distribuição
- Relacionamento e apoio ao cliente em contexto de segurança digital
- Modelo de subscrição vs pagamento único

- Papel das parcerias tecnológicas e reputação de marca
- Articulação entre funcionalidade e percepção de valor (incluindo tamanho e usabilidade do dispositivo)

Estes tópicos foram sistematizados e transformados em questões dirigidas para a 2.^a sessão, com base na metodologia do Business Model Canvas.

2.^a Sessão – Discussão Estruturada e Validação Qualitativa

Objetivo da Sessão:

Validar, através de discussão orientada, os elementos-chave do modelo de negócio Canvas do KIS com base nos tópicos identificados na sessão anterior, através de perguntas específicas e cenários simulados.

Duração Aproximada: 2 horas

Resumo dos Tópicos e Questões Abordadas:

- 1. Lembrar o dispositivo e funcionalidades**
- 2. Concorrência e posicionamento**
- 3. Segmentos de clientes**

Questão colocada aos participantes:

“Considera viável deter um segmento de clientes híbrido (B2C + B2B)?”

- 4. Canais de distribuição**

Questões colocadas aos participantes:

“Em que contexto ou ambiente se sentiria mais seguro e confiante para adquirir um dispositivo como o KIS (online ou em loja física)?”

“Que fatores considera que iriam suportar a confiança através da compra no canal online?”

- 5. Relacionamento com o cliente**

Questões colocadas aos participantes:

“O que esperaria de uma marca que lhe promete segurança total dos seus acessos e ativos digitais?”

“Implementaria algum elemento diferente?”

6. Fontes de receita

Questões colocadas aos participantes:

“Que tipo de serviço adicional justificaria, na sua opinião, uma subscrição mensal associada ao KIS?”

“Na sua opinião, faria mais sentido pagar um valor único mais elevado ou um valor base mais acessível com serviços adicionais por subscrição?”

7. Recursos-chave e parceiros

Questões colocadas aos participantes:

“Na sua opinião, quais são os recursos essenciais para garantir confiança num modelo de negócio baseado em segurança digital e proteção de dados?”

“Considera que as parcerias tecnológicas aumentam a perceção de confiança no negócio ou são excessivas?”

8. Atividades-chave

Questão colocada aos participantes:

“Na sua opinião, estas atividades-chave serão suficientes?”

9. Proposta de valor (com personas e simulação de contexto de uso)

Personas apresentadas:

Sofia Marques (utilizadora pessoal – B2C)

João Ribeiro (diretor de sistemas de informação – B2B)

Questões colocadas aos participantes:

“O que consideram útil?”

“O que vos parece confuso ou desnecessário?”

“Que funcionalidades sentem que estão em falta?”

Metodologia:

- Apresentação sintética com apoio de slides
- Discussão orientada com questões por tópico
- Registo integral da sessão (transcrição)
- Análise qualitativa dos contributos para posterior reformulação do modelo

Encerramento

Síntese dos contributos obtidos, agradecimento formal aos participantes e indicação de que os resultados da sessão seriam utilizados para aperfeiçoar o plano de negócios e a proposta de valor do dispositivo KIS