INSTITUTO
UNIVERSITÁRIO
DE LISBOA

# Um Estudo de Caso em Cabo Verde com Utilização de Privacidade de Dados

Hénio do Rosário de Pina

Mestrado em Informática e Gestão

Orientador:
Doutor Valderi Reis Quietinho Leithardt, Professor Auxiliar (com Agregação),
Iscte – Instituto Universitário de Lisboa

Orientador:
Doutor Sérgio Miguel Carneiro Moro, Professor Catedrático,
Iscte – Instituto Universitário de Lisboa

Julho, 2026

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciência e Tecnologia da Informação

# Um Estudo de Caso em Cabo Verde com Utilização de Privacidade de Dados

Hénio do Rosário de Pina

Mestrado em Informática e Gestão

Orientador:
Doutor Valderi Reis Quietinho Leithardt, Professor Auxiliar (com Agregação),
Iscte – Instituto Universitário de Lisboa

Orientador:
Doutor Sérgio Miguel Carneiro Moro, Professor Catedrático,
Iscte – Instituto Universitário de Lisboa

Julho, 2026

*Se não puder voar, Corra.*
*Se não puder correr, ande.*
*Se não puder andar, rasteje, mas*
*continue em frente de qualquer jeito."*
*Martin Luther King Jr.*

# Agradecimentos

Em primeiro lugar, agradeço a Deus por iluminar e guiar os meus passos em cada momento desta jornada.

A minha esposa, Yasmin Mártir, agradeço profundamente pela parceria, pelo companheirismo, pelo apoio constante e pela troca de experiências ao longo deste percurso. Sua colaboração foi fundamental.

Aos meus filhos, Hania, Hiago e Héron, a minha eterna gratidão por serem a minha maior motivação e inspiração para seguir em frente, mesmo nos momentos mais difíceis.

Aos meus pais, as minhas irmãs e aos meus sobrinhos, o meu mais sincero agradecimento por nunca medirem esforços para que eu chegasse até aqui.

Um agradecimento muito especial aos meus orientadores, professor Valderi Leithardt e o professor Sérgio Moro pela paciência, dedicação, incentivo e energia positiva que sempre me transmitiram.

# Resumo

A dissertação tem como objetivo o desenvolvimento e a avaliação de uma solução tecnológica para o ecossistema do turismo cabo-verdiano, incorporando os princípios de privacidade e de proteção da informação desde a fase de concepção. Para o efeito, foi adotada a metodologia Design Science Research, que sustentou a fundamentação teórica, desenvolvimento do protótipo e a sua posterior avaliação. A plataforma digital proposta incorpora as ferramentas de segurança, privacidade e proteção de dados do turista, que adota os princípios de *Privacy by Design e Privacy by Default*. A avaliação foi realizada em ambiente controlado; ainda assim, demonstrou que o protótipo cumpre os requisitos funcionais e não funcionais propostos. Os resultados obtidos demonstram que o protótipo tem grande potencial para diminuição dos riscos quanto ao tratamento de dados pessoais, que é fundamental para o reforço da confiança digital dos usuários no turismo. Ainda assim, o estudo apresenta limitações, principalmente por falta de uma validação no ambiente real, o que limita realizações de testes em vários cenários, que será importante fazer numa investigação futura. De forma geral, a dissertação demonstra que a integração da privacidade desde a fase de concepção não é só possível, como é indispensável para o desenvolvimento de sistemas digitais mais seguros e em conformidade com o normativo legal.

**Palavras-chave:** Privacidade de dados; *design science research; privacy by design*; Cabo Verde.

# Abstract

This dissertation aims to develop and evaluate a technological solution for the Cape Verdean tourism ecosystem, incorporating the principles of privacy and information protection from the design phase. To this end, the Design Science Research methodology was adopted, which underpinned the theoretical foundation, prototype development, and its subsequent evaluation. The proposed digital platform incorporates security, privacy, and tourist data protection tools, adopting the principles of Privacy by Design and Privacy by Default. The evaluation was conducted in a controlled environment; even so, it demonstrated that the prototype meets the proposed functional and non-functional requirements. The results obtained demonstrate that the prototype has great potential for reducing risks related to the processing of personal data, which is fundamental for strengthening users' digital trust in tourism. However, the study presents limitations, mainly due to a lack of validation in a real-world environment, which limits testing in various scenarios, something that will be important in future research. In general, the dissertation demonstrates that integrating privacy from the design phase is not only possible but indispensable for the development of more secure digital systems in compliance with legal regulations.

**Keywords**: Data privacy; design science research; privacy by design; Cape Verde.

# Índice

**Agradecimentos** ..... i

**Resumo** ..... iii

**Abstract** ..... v

**Lista de Figuras** ..... x

**Lista de Tabelas** ..... xi

**Lista de abreviação e acrónimos** ..... xii

**CAPÍTULO 1** ..... 1

**Introdução** ..... 1

**1.1 Motivação** ..... 2

**1.2 Objetivo da Investigação** ..... 2

**1.3 Metodologia** ..... 3

**Revisão da Literatura** ..... 5

**2.1 Design Science Research** ..... 5

**2.5 Turismo em Cabo Verde** ..... 7

**2.6 Dados Pessoais no Setor do Turismo** ..... 9

**2.7. Conceito da Privacidade** ..... 10

**2.8. Conceito Proteção de Dados** ..... 10

**2.9. Conceito Dados Pessoais** ..... 10

**2.10. Princípios da Privacidade de Dados** ..... 10

**2.11. Privacidade no Contexto Computação Quântica: Desafios e perspetivas atuais** ..... 11

**2.11.1. Ameaças à Privacidade Causados pela Computação Quântica** ..... 12

**2.11.2. Oportunidade e Mecanismo Quânticos para Proteger a Privacidade** ..... 12

**2.12. Privacy by Design e Privacy by Default** ..... 12

**2.13. Enquadramento Comparativo entre o Regime de Proteção de Dados de Cabo Verde e Portugal/UE** ..... 12

**2.13.1. Quadros Comparativos da Legislação Cabo-Verdiana e Portuguesa/EU** ..... 14

**CAPÍTULO 3** ..... 16

**Metodologia de Investigação** ..... 16

**3.1 Abordagem Metodológica** ..... 16

**3.2 Ciclos da Design Science Research** ..... 16

**3.2.1 Ciclo de Relevância** ..... 17

**3.2.2 Ciclo de Rigor** ..... 17

**3.2.3 Ciclo de Engenharia** ..... 17

**3.3 Métodos de Recolha de Dados** ..... 18

**3.4 Critérios de Avaliação do Artefacto** ..... 18

**CAPÍTULO 4** ..... 20

**Análise e a Identificação dos Requisitos** ..... 20

**4.1 Identificação de Stakeholders** ..... 20

**4.2 Levantamento de Requisitos Funcionais / Requisitos Não Funcionais** ..... 21

**4.3 Requisitos de Privacidade e Proteção de Dados** ..... 22

**4.3.1 Requisitos da base legal aplicável** ..... 22

**4.3.2 Requisitos técnicos** ..... 23

**4.3.3 Requisitos organizacionais** ..... 24

**4.4 Diagramas de Casos de Uso** ..... 25

**4.4.1 Descrição de Caso de Uso** ..... 25

**CAPÍTULO 5** ..... 32

**Concepção e desenvolvimento do Protótipo** ..... 32

**5.1 Introdução ao Protótipo** ..... 32

**5.2 Arquitectura do Protótipo** ..... 32

**5.2.1 Desenho da Interface do Utilizador** ..... 32

**5.2.2 Camada de Lógica de Negócio - Backend** ..... 33

**5.2.3 Camada de Gestão de Dados** ..... 33

**5.2.4 Camada de Auditoria e Conformidade** ..... 34

**5.3 Princípios de Privacidade Integrados** ..... 35

**5.3.1 Privacy by Design** ..... 35

**5.3.2 Privacy by Default** ..... 36

**5.4 Integração do Modelo Oraculum na Gestão de Privacidade** ..... 37

**5.5 Modelação do Sistema** ..... 38

**5.5.1 Diagramas Conceptuais** ..... 38

**5.6 Ciclo de Vida do Tratamento de Dados Pessoais** ..... 39

**5.7 Implementação do Protótipo** ..... 41

**5.8 Especificação Técnica do Protótipo** ..... 48

**CAPÍTULO 6** ..... 49

**Avaliação do Protótipo** ..... 49

**6.1 Enquadramento da Avaliação do Protótipo** ..... 49

**6.2 Metodologia de Avaliação** ..... 50

**6.2.1 Abordagem Metodológica** ..... 50

**6.2.2 Instrumentos de Recolha de Dados** ..... 50

**6.2.3 Participantes** ..... 51

**6.2.4 Procedimento de avaliação** ..... 51

**6.2.5 Técnicas de análise de dados** ..... 51

**6.3 Caracterização da Amostra** ..... 52

**6.3.1 Faixa etária** ..... 52

**6.3.2 Género** ..... 53

**6.3.3 Formação Académica** ..... 54

**6.4 Análise Descritiva dos Resultados** ..... 54

**6.4.1 Perceção sobre privacidade e proteção de dados** ..... 55

**6.4.2 Avaliação do protótipo** ..... 55

**6.4.3 Avaliação global do protótipo** ..... 58

**6.5 Consistência Interna do Instrumento** ..... 58

**6.6 Análise Qualitativa da Respostas Abertas** ..... 59

**6.6.1 Aspectos positivos** ..... 59

**6.6.2 Sugestões de melhorias** ..... 59

**Capítulo 7** ..... 60

**Conclusões e recomendações** ..... 60

**7.1 Principais conclusões** ..... 60

**7.2 Limitações do Estudo** ..... 61

**7.3 Recomendações para Investigação Futura** ..... 61

**7.4 Considerações Finais** ..... 61

**REFERÊNCIA BIBLIOGRÁFICA** ..... 63

**ANEXO** ..... 66

**Anexo A- Política de Privacidade** ..... 66

**Anexo B Questionário** ..... 69

**Anexo C – Carta de Aceite** ..... 73

# Lista de Figuras

**Figura 1 - As ilhas de Cabo Verde** ..... 7
**Figura 2 - Localização geográfica de Cabo Verde** ..... 9
**Figura 3 - Principais mercados emissores do turismo 3º Trimestre 2025 (INE,2025)** ..... 9
**Figura 4 - Ciclo DSR**.....17
**Figura 5 - Ciclo empírico** .....17
**Figura 6 - Ciclo de engenharia**.....18
**Figura 7 - Interação dos atores com o sistema na Visão Global**.....25
**Figura 8 - Modelo Integrado de Governação da Privacidade** .....35
**Figura 9 - Página inicial do protótipo GoCaboVerde**.....42
**Figura 10 - Interface de pesquisa e consulta de tours**.....43
**Figura 11 - Interface de criação de conta e aceitação das condições de tratamento de dados..**43
**Figura 12 - Interface de autenticação do utilizador**.....44
**Figura 13 - Área de perfil e gestão dos dados pessoais do utilizador** .....45
**Figura 14 - Interface de gestão da privacidade e do consentimento**.....45
**Figura 15 - Interface para o exercício dos direitos do titular dos dados** .....46
**Figura 16 - Interface para comunicação de incidentes** .....47
**Figura 17 - Distribuição da amostra por faixa etária.** .....53
**Figura 18 - Distribuição da amostra por género** .....53
**Figura 19 - Distribuição da amostra por habilitações académicas**.....54

# Lista de Tabelas

**Tabela 1 - Princípios fundamentais da proteção de dados** ..... 14
**Tabela 2 - Direitos dos titulares dos dados** ..... 15
**Tabela 3 - Obrigações das entidades responsáveis pelo tratamento** ..... 15
**Tabela 4 - Privacy by design e Privacy by default** ..... 15
**Tabela 5 - Relevância para o sector do turismo** ..... 15
**Tabela 6 - Processo metodológico baseado em Design Science Research** ..... 16
**Tabela 7 - Requisitos funcionais e Comportamento esperado do sistema** ..... 21
**Tabela 8 - Requisitos não funcionais** ..... 22
**Tabela 9 - Caso de uso de Registo de utilizador** ..... 26
**Tabela 10 - Caso de uso de Autenticação de utilizador** ..... 26
**Tabela 11 - Caso de uso de Gestão de perfil de utilizador** ..... 27
**Tabela 12 - Caso de uso de Pesquisa de serviços turísticos** ..... 27
**Tabela 13 - Caso de uso de Reservar serviço turístico** ..... 28
**Tabela 14 - Caso de uso de Gestão de consentimento** ..... 28
**Tabela 15 - Caso de uso de Gestão de direitos do titular** ..... 29
**Tabela 16 - Caso de uso Reportar incidente** ..... 29
**Tabela 17 - Caso de uso de Gestão de utilizadores** ..... 30
**Tabela 18 - Caso de uso de Gestão de perfil e controlo de acesso** ..... 30
**Tabela 19 - Caso de uso Monitorizar incidentes** ..... 31
**Tabela 20 - Distribuição da amostra por faixa etária** ..... 52
**Tabela 21 - Distribuição da amostra por género** ..... 53
**Tabela 22 - Distribuição da amostra por habilitações académicas** ..... 54
**Tabela 23 - Médias da Dimensão Perceção sobre Privacidade e Proteção de Dados** ..... 55
**Tabela 24 - Resultados da dimensão Usabilidade** ..... 56
**Tabela 25 - Resultados da dimensão Transparência e Privacidade** ..... 56
**Tabela 26 - Resultados da dimensão Confiança** ..... 57
**Tabela 27 - Resultados da dimensão Intenção de Uso** ..... 57
**Tabela 28 - Médias da Dimensão Avaliação Global do Protótipo** ..... 58
**Tabela 29 - Resultados do Coeficiente Alpha de Cronbach** ..... 59

## Lista de abreviação e acrónimos

**CNPD-CV -** Comissão Nacional de Proteção de Dados de Cabo Verde

**CSS3** - Cascading Style Sheets

**DPIA -** Data Protection Impact Assessment

**DSR –** Design Science Research

**GB** - Gigabyte

**GSTC -** Global Sustainable Tourism Council

**HTML -** HyperText Markup Language

**IoT -** Internet of Things

**ISCTE-IUL -** Instituto Universitário de Lisboa

**INE -** Instituto Nacional de Estatísticas

**MFA -** Multi-Factor Authentication

**RAM -** Random Access Memory

**RBAC -** Role-Based Access Control

**RGPD** - Regulamento Geral sobre a Proteção de Dados

**TIC –** Tecnologias da informação e comunicação

**TLS -** Transport Layer Security

**EU –** European Union

**UGPE –** Unidade de Gestão de Projetos Especiais

## CAPÍTULO 1

# Introdução

A transformação digital tem sido essencial no desenvolvimento e na estratégia no turismo, promovendo adaptações nos modelos de negócio, nos processos e nas formas de articulação entre as organizações do setor e o turista. De acordo com (Barbosa & Medaglia, 2020) o aumento da utilização das plataformas digitais tem permitido uma maior eficiência na gestão, bem como nos serviços personalizados, baseada na recolha e análise de dados pessoais dos turistas. Na era digital em que vivemos, somos testados quanto à privacidade e proteção da informação.

Com o novo comportamento do turista, ela através de novas culturas ou de experiências novas, os seus dados pessoais são cada vez mais armazenados e utilizados no setor do turismo. Com essa necessidade de as organizações recolherem os dados pessoais, originou-se uma grande preocupação com a privacidade de dados na era digital e como eles são tratados, principalmente junto dos turistas internacionais (Ioannou et al., 2021).

A intensificação do uso de dados pessoais no setor do turismo gera uma preocupação no domínio da privacidade e da proteção de dados. A recolha, o tratamento e o armazenamento de informação sensível, associados à personalização de serviços e produtos turísticos, colocam exigências acrescidas às organizações no que respeita ao cumprimento de princípios éticos, legais e de segurança da informação. A gestão errada da privacidade pode comprometer a confiança dos turistas, afetar a reputação das organizações e pôr em causa a sustentabilidade e desenvolvimento turístico (Preko et al., 2025).

Cabo Verde é uma economia insular em desenvolvimento médio, o turismo é visto como um eixo estratégico para o crescimento económico. Pode-se verificar o crescimento do turismo nos últimos anos, através de um aumento do número de turistas, do montante de receitas, do número de hóspedes e da geração de emprego. Então a utilização de soluções digitais que geram confiança assume uma particular importância.

A presença digital dos operadores turísticos e a utilização de soluções tecnológicas inovadoras têm acompanhado o crescimento do setor, tornando a utilização de dados pessoais um recurso estratégico para a melhoria da experiência do turista e para o aumento da promoção e competitividade do destino.

Apesar do crescente impacto da privacidade de dados no espaço do turismo digital, verifica-se uma falha na literatura no que diz respeito ao estudo baseado em dados reais destas questões em economias insulares, em particular no arquipélago cabo-verdiano.

Nesta senda, o estudo propõe o desenvolvimento de uma plataforma digital direcionada ao setor turístico de Cabo Verde, desenvolvida de acordo com os princípios de proteção de dados desde a fase inicial. A investigação procura não apenas responder a desafios técnicos, mas também contribuir para uma abordagem mais integrada entre inovação tecnológica e a conformidade normativa e legal, adotando a metodologia DSR.

## 1.1 Motivação

No mundo atual de tecnologias digitais aplicadas ao turismo, vê-se que muitas soluções tecnológicas, especialmente os aplicativos móveis, não usam de forma eficaz os princípios de privacidade e proteção de dados desde a fase inicial do desenvolvimento do protótipo. Geralmente, a privacidade é tratada apenas para cumprimento e conformidade legal mínima (Cejas et al., 2025).

Atendendo à importância do turismo para Cabo Verde, principalmente ao turismo internacional, a plataforma turística desenvolvida estará de acordo com as legislações e normas cabo-verdianas, Regulamento Geral de Proteção de Dados de Portugal e da União Europeia. A inexistência de soluções digitais comprometidas com a privacidade de dados pode comprometer a confiança dos turistas, expor as organizações a riscos jurídicos legais e limitar a sustentabilidade do turismo digital.

Perante este cenário, propõe-se a seguinte questão de investigação: como desenvolver e avaliar um protótipo turístico incorporando os princípios de privacidade e proteção de dados, tendo em conta o turismo digital em Cabo Verde e as referenciais normativas nacionais e internacionais aplicáveis?

## 1.2 Objetivo da Investigação

Este estudo propõe um aplicativo turístico baseado na privacidade e proteção de dados, fundamentado nos princípios de Privacy by Design e Privacy by Default, para turismo digital de Cabo Verde, alinhado com as preocupações dos turistas de como são tratados e organizados os seus dados pessoais em conformidade com o RGPD, as orientações da CNPD-CV e as boas práticas internacionais em privacidade digital (Cavoukian, 2020).

Os objetivos específicos incluem:

1. Analisar a literatura científica sobre privacidade e proteção de dados e confiança dos turistas no turismo digital;
2. Levantamento dos requisitos de privacidade e proteção de dados com base em CNPD-CV, RGPD e boas práticas internacionais de proteção de dados;
3. Aplicar a metodologia Design Science Research (DSR) para o desenvolvimento de um protótipo tecnológico, assegurando uma abordagem científica, orientada à resolução de problemas reais (Silveira & Reis, 2022);
4. Desenvolver um modelo conceitual de aplicativo turístico centrado na proteção de dados pessoais, baseado nos princípios de Privacy by Design e Privacy by Default desde a fase de concepção (Cavoukian, 2020);
5. Avaliar a qualidade do protótipo proposto quanto à sua utilização pelos utilizadores e ao cumprimento dos requisitos de privacidade identificados.

### 1.3 Metodologia

A investigação em Sistemas de Informação pode ser abordada em pontos de vista diferentes, de um lado com objetivo na explicação de acontecimento e, de outro, focados em desenvolvimento de criação de soluções. Nesta pesquisa, a Design Science Research destaca-se por desenvolver um protótipo com o objetivo de resolver os problemas identificados (Hevner et al., 2004).

A Design Science Research não só se centraliza na abordagem explicativa, mas sim se inicia a partir de um problema identificado e, com base nisso, desenvolve soluções tecnológicas que, por sua vez, serão avaliadas. O conhecimento produzido não é só o resultado da análise teórica, mas também da aplicação desenvolvida e da sua validação.

A metodologia organiza-se em três dimensões fundamentais. Onde o problema se manifesta ou ocorre, a base científica que sustenta a parte teórica e o desenvolvimento do protótipo. Desta forma, assegura-se que o protótipo desenvolvido não é apenas inovador, mas com fundamentação teórica e com valor social (Hevner et al., 2024).

A dissertação organiza-se da seguinte forma: o Capítulo 1 apresenta a motivação, as questões de investigação, os objetivos e as metodologias escolhidas; o Capítulo 2 apresenta a fundamentação teórica; o Capítulo 3 mostra a metodologia de investigação; o Capítulo 4 apresenta a análise do contexto e identificação dos requisitos; o Capítulo 5 apresenta concepção e desenvolvimento do protótipo; o Capítulo 6 apresenta à avaliação do protótipo de acordo com

a metodologia aplicado e, por fim, o Capítulo 7 apresenta as conclusões e propostas de trabalhos futuros.

Está investigação visa contribuir para o desenvolvimento do turismo cabo-verdiano através da proposta de um modelo de protótipo que incorpora requisitos legais e as normas de CNPD-CV e RGPD-EU desde a fase de concepção.

# CAPÍTULO 2

# Revisão da Literatura

## 2.1 Design Science Research

A investigação em Sistemas de Informação pode ser abordada em pontos de vista diferentes, de um lado com objetivo na explicação de acontecimento e, de outro, focados em desenvolvimento de criação de soluções. Nesta pesquisa, a Design Science Research destaca-se por desenvolver um protótipo com o objetivo de resolver o problema identificado (Hevner, 2007).

A Design Science Research não só se centraliza na abordagem explicativa, mas sim se inicia a partir de um problema identificado e, com base nisso, desenvolve soluções tecnológicas que, por sua vez, serão avaliadas. O conhecimento produzido não é só o resultado da análise teórica, mas também da aplicação desenvolvida e da sua validação.

A metodologia organiza-se em três dimensões fundamentais. Onde o problema se manifesta ou ocorre, a base científica que sustenta a parte teórica e o desenvolvimento do protótipo. Desta forma, assegura-se que o protótipo desenvolvido não é apenas inovador, mas com fundamentação teórica e com valor social (Peffers et al., 2007).

## 2.2 Transformação Digital no Turismo

Com a evolução da tecnologia de forma transversal, as operações que eram feitas de forma manual no turismo passaram a ser realizadas através de plataformas digitais. Por exemplo, uma simples reserva atualmente faz-se por meio da aplicação. Esta transformação não se restringe só à melhoria dos processos, mas permite reajustamento dos serviços e das preferências dos turistas de acordo com as análises de dados recolhidos. Segundo a análise feita, pode-se afirmar que as experiências turísticas estão cada vez mais ajustadas às necessidades do turista. Quanto maior é o sistema automatizado, maior é a necessidade da recolha e processamento de dados pessoais. A competitividade dos destinos passa a estar associada à sua capacidade de gerir informação de forma estratégica, mas também responsável (Ordóñez-Martínez et al., 2024).

Conforme indicam os estudos recentes, vários destinos turísticos europeus têm vindo a desenvolver ecossistemas digitais complexos, que interagem com diversas fontes de dados, com a finalidade de otimização de gestão dos destinos e apoio a processos de decisão (Gretzel et al., 2015). Nesta abordagem, a tecnologia assume um papel estratégico, e não só na melhoria da eficiência dos processos das entidades envolvidas, mas também na transformação da experiência turística, cada vez mais sujeita às análises de dados realizadas com as informações recolhidas das experiências dos turistas e que em seguida são mapeadas pelo sistema.

Contudo, a crescente utilização de informação pessoal do turista por parte da indústria turística tem impactado novos desafios, principalmente na vertente de segurança da informação. Torna-se fundamental que as organizações tenham a capacidade de uma gestão ética e responsável da privacidade dos dados, comprometendo-se a proteger a informação para que não seja usada de forma abusiva.

Assim, uma conjugação entre a evolução tecnológica e a gestão ética e correta dos dados pessoais gera um fator determinante para a promoção organizacional e à confiança dos utilizadores.

### 2.3 Transformação Digital no Contexto Turístico de Cabo Verde

O território cabo-verdiano tem registado um aumento no acesso à internet e à tecnologia de informação nos últimos anos. Essa evolução digital das ilhas de Cabo Verde em relação ao resto do mundo tem um impacto bastante positivo, promovendo o país em plataformas digitais, consolidando Cabo Verde como um destino turístico (Kemp, 2025).

O mapeamento digital das ilhas no projeto, como Google Street View, é fundamental para aumentar a visibilidade internacional de Cabo Verde, o que acaba por atrair mais turistas e investidores. Esta solução reduz a escassez da informação sobre o país, o que acaba por impulsionar a economia local, tornando-se uma ferramenta estratégica para as pequenas e médias empresas do setor de turismo, como hotelaria, restauração e outros, ao conferir maior visibilidade aos negócios (A Semana/InforPress, 2025).

Em economias como a cabo-verdiana em que o turismo assume um papel estratégico, a confiança e credibilidade das plataformas digital são cruciais para o uso dos utilizadores. Assim, a integração de medidas e práticas de privacidade e proteção da informação desde a fase inicial do desenvolvimento da plataforma é essencial para assegurar a viabilidade e a confiança digital dos utilizadores.

## 2.4 Caracterização de Cabo Verde

Cabo Verde, localizado no Oceano Atlântico Norte, a cerca de 500 quilómetros da costa ocidental africana, composto por dez ilhas de origem vulcânica, com características geográficas, ambientais e culturais distintas entre as ilhas (Pires Silva Mendonça Orientação & Barros Matos, 2018). A diversidade das ilhas possibilita diversas formas de turismo, incluindo o turismo de praia, rural e da montanha (Instituto do Turismo de Cabo Verde, 2018).

Cabo Verde era uma colônia portuguesa e apenas alcançou a sua independência em 1975. Atualmente, destaca-se pela estabilidade política e pela valorização da sua identidade cultural, fatores que reforçam a sua atratividade enquanto destino turístico (Almeida & Salvador, 2003).

Apesar das vantagens competitivas, a característica insular acrescenta desafios específicos, tanto ao nível da dependência económica de setores estratégicos como o turismo, transporte e outros. Esta dependência reforça a necessidade de adoção de estratégias sustentáveis que garantam o equilíbrio entre crescimento econômico e preservação dos recursos locais.




***Figura 1 - As ilhas de Cabo Verde***

***Fonte: Wikipédia. Geografia de Cabo Verde. Disponível em: https://pt.wikipedia.org/wiki/Geografia_de_Cabo_Verde. Acesso em: 15 out. 2025.***

## 2.5 Turismo em Cabo Verde

As ilhas de Cabo Verde são um destino ímpar, uma vez que, por causa da sua natureza, possuem uma temperatura amena durante todo o ano, além de uma identidade cultural, musical e uma oferta distintiva na gastronomia, o que molda a experiência do visitante. Pela sua localização privilegiada entre os continentes americano e europeu, além de um ambiente seguro e estabilidade social e política. Assim, o país se coloca de maneira estratégica internacionalmente.

A conexão aérea é um elemento fundamental na dinâmica do setor, sustentada por quatro aeroportos internacionais (Instituto do Turismo de Cabo Verde, 2018).

Em Cabo Verde, o turismo tem um papel crucial no desenvolvimento da economia. O setor é responsável por uma parte significativa do produto interno bruto, o que evidencia a sua importância económica e social do país, o que promove a diversificação e modernização da economia (Ministério das Finanças de Cabo Verde, 2025). A intenção não é apenas um aumento quantitativo, mas sim, essa estratégia deve ter como objetivo a melhoria da qualidade de vida dos cidadãos cabo-verdianos, o equilíbrio das contas externas e a geração de emprego qualificado, metas essas que estão alinhadas com as prioridades do governo e os programas de financiamento internacional, que buscam tornar o setor mais resiliente, diversificado e inserido em cadeias de valor que beneficiem as comunidades locais (Unidade de Gestão de Projetos Especiais, 2023).

Neste sentido, o Programa Operacional de Turismo estabelece as diretrizes com foco que visa definir uma rede bem estruturada de produtos turísticos. Esta estratégia tem como missão tornar Cabo Verde um destino turístico até 2030, com o objetivo de repartir os benefícios por todas as ilhas de forma equitativa. Assim, desta forma, conquistando a confiança do setor e trabalhando em conjunto para reforçar as suas condições de competitividade turística.

É fundamental que este crescimento ocorra em conjugação entre a preservação ambiental e o respeito pela identidade cultural cabo-verdiana. A adoção de normas nacionais em conformidade com padrões internacionais de turismo sustentável, como os critérios de sustentabilidade para alojamento, operadores e destinos reconhecidos em 2023 pelo Global Sustainable Tourism Council, salienta o compromisso do país com práticas que protejam os recursos naturais e culturais enquanto promovem uma experiência turística (Global Sustainable Tourism Council, 2023).




***Figura 2 - Localização geográfica de Cabo Verde***

***Fonte: Cabo Verde Airlines, 2019, citado por AEROIN, Acesso em: 15 out. 2025***

| País de residência habitual | Santo Antão | São Vicente | São Nicolau | Sal | Boa Vista | Maio | Santiago | Fogo | Brava | Total | % |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cabo Verde** | **4 141** | **8 102** | **1 003** | **6 218** | **1 692** | **1 272** | **11 307** | **1 735** | **490** | **35 960** | **2,5** |
| **Estrangeiro** | **10 159** | **17 974** | **765** | **824 364** | **522 838** | **1 281** | **40 014** | **5 955** | **680** | **1 424 030** | **97,5** |
| Reino Unido | 124 | 138 | 12 | 238 854 | 271 975 | 8 | 441 | 34 | 12 | **511 598** | **35,0** |
| Portugal | 632 | 3 400 | 87 | 196 608 | 51 078 | 56 | 9 864 | 1 182 | 14 | **262 921** | **18,0** |
| Alemanha | 759 | 710 | 59 | 50 296 | 64 755 | 44 | 1 306 | 458 | 24 | **118 411** | **8,1** |
| Espanha | 1 277 | 1 728 | 18 | 64 088 | 18 976 | 136 | 2 651 | 665 | 75 | **89 614** | **6,1** |
| Polónia | - | 18 | - | 68 626 | 17 680 | - | 101 | - | - | **86 425** | **5,9** |
| Belgica+Holanda | 1 338 | 2 676 | 214 | 39 813 | 30 865 | 195 | 1 707 | 150 | 43 | **77 001** | **5,3** |
| França | 4 150 | 4 687 | 104 | 30 719 | 21 706 | 450 | 5 281 | 1 894 | 214 | **69 205** | **4,7** |
| Italia | 62 | 214 | 8 | 24 765 | 12 731 | 232 | 745 | 145 | 93 | **38 995** | **2,7** |
| Eslováquia | - | - | - | 3 529 | 7 828 | - | - | - | - | **11 357** | **0,8** |
| Estados Unidos | 54 | 1 045 | 55 | 2 473 | 763 | 4 | 3 417 | 724 | 162 | **8 697** | **0,6** |
| Suiça | 126 | 419 | 192 | 3 648 | 717 | - | 1 231 | 486 | 18 | **6 837** | **0,5** |
| Austria | 27 | 40 | - | 1 593 | 1 882 | - | 96 | 22 | - | **3 660** | **0,3** |
| Luxemburgo | - | 156 | - | 2 698 | 120 | - | 218 | - | - | **3 192** | **0,2** |
| Senegal | - | 44 | - | 974 | 3 | - | 2 024 | - | - | **3 045** | **0,2** |
| Roménia | - | 8 | - | 1 071 | 1 416 | - | 40 | - | - | **2 535** | **0,2** |
| Irlanda | - | 6 | - | 1 246 | 933 | - | 54 | - | - | **2 239** | **0,2** |
| Marrocos | - | 11 | - | 490 | 32 | - | 853 | - | - | **1 386** | **0,1** |
| Brasil | - | 55 | - | 450 | 372 | - | 280 | - | - | **1 157** | **0,1** |
| Angola | - | 47 | - | 87 | 21 | - | 922 | - | - | **1 077** | **0,1** |
| Nigéria | - | - | - | 395 | 6 | - | 494 | - | - | **895** | **0,1** |
| Outros Paises | 1 610 | 2 572 | 16 | 91 941 | 18 979 | 156 | 8 289 | 195 | 25 | **123 783** | **8,5** |
| **Total** | **14 300** | **26 076** | **1 768** | **830 582** | **524 530** | **2 553** | **51 321** | **7 690** | **1 170** | **1 459 990** | **100,0** |
| **%** | **1,0** | **1,8** | **0,1** | **56,9** | **35,9** | **0,2** | **3,5** | **0,5** | **0,1** | **100,0** | |

***Figura 3 - Principais mercados emissores do turismo 3º Trimestre 2025 (INE,2025)***

## 2.6 Dados Pessoais no Setor do Turismo

Atualmente, o turismo depende em larga escala das recolhas e utilização dos dados pessoais de turistas. Com as mesmas informações recolhidas, pode-se ajustar os serviços para que sejam personalizados. No entanto, com o aumento brutal e a variedade desses dados, aumenta o risco caso não haja mecanismo de proteção eficazes. Assim, é fundamental implementar políticas estratégicas que garantam segurança e promoção da gestão responsável da informação ao longo do ciclo de vida dos dados.

Estudos recentes alertam para a complexidade legal e operacional de tratar dados pessoais na indústria turística e apontam para lacunas na implementação das normas de proteção de dados em plena conformidade com os requisitos legais, bem como para a necessidade de

medidas de segurança reforçadas para evitar acessos não autorizados e mau uso de informação sensível (Sonja Lucic, 2023).

### 2.7. Conceito da Privacidade

A privacidade é o direito de uma pessoa de controlar suas informações pessoais. No ambiente digital, é mais complexo, pois não se trata apenas de armazenar os dados, mas também de conceder a outros o privilégio de recolha e poder de manipulá-los. A crescente recolha e análise de dados, impulsionada pela automação dos sistemas, tem causado um debate em torno da privacidade. A privacidade assume um papel estruturante na proteção da dignidade humana, da liberdade de escolha e da autonomia informativa (Powell, 2025).

### 2.8. Conceito Proteção de Dados

A proteção de dados são as regras e maneiras de agir no contexto de informações pessoais. Tem o objetivo de assegurar que os dados sejam utilizados de forma segura e clara. Estas normas buscam equilibrar a utilização de dados para fins tecnológicos e comerciais. Este enquadramento não visa impedir a inovação tecnológica, mas assegurar que a utilização de dados ocorre dentro de parâmetros definidos, equilibrando interesses económicos e direitos fundamentais (Regulamento (UE) 2016/679).

### 2.9. Conceito Dados Pessoais

São informações relativas a uma pessoa singular identificada ou identificável (Regulamento (UE) 2016/679, art. 4.º). Uma pessoa é identificável quando pode ser reconhecida direta ou indiretamente, por exemplo, através de um nome, número, características físicas, dados eletrónicos ou outros elementos que permitam a sua identificação.

Em turismo, a identificação do titular dos dados ocorre, com mais frequência, de forma direta, o que traz um alto nível de responsabilidade por parte das organizações que realizam o tratamento dos dados.

### 2.10. Princípios da Privacidade de Dados

Os princípios da privacidade e proteção de dados constituem um conjunto de normas que orientam o tratamento ético da informação. Este princípio reforça a transparência no tratamento

de dados, assegurando que apenas o que é necessário seja recolhido e que as informações sejam precisas e atualizadas. É importante que a sua conservação seja apenas por um tempo estritamente necessário e que a segurança e a confidencialidade estejam garantidas (RGPD, 2016; CNPD-CV). Estes princípios são fundamentais para garantir que os titulares dos dados possam exercer de forma plena os seus direitos, o que será fundamental para reforçar a confiança nas organizações que operam no ambiente digital, especialmente na indústria do turismo.

Além das diretrizes estabelecidas na legislação de proteção de dados, a literatura académica tem se dedicado às técnicas que permitem a incorporação da privacidade no desenvolvimento de plataformas digitais. Portando, (Silva et al., 2019) recomendam que o requisito de privacidade seja ajustado de acordo com o perfil de uso, o ambiente em que o sistema está integrado e a hierarquia de acesso.

Com isso,(Leithardt et al., 2020), propõem uma proposta de abordagem middleware que ajusta permissões e acessos de acordo com a frequência de uso e a interação com a plataforma. Este modelo permite a disponibilização de informação de acordo com o ambiente e as regras contextuais definidas, promovendo uma gestão mais flexível e contextualizada da privacidade em sistemas digitais.

Estas abordagens evidenciam a importância de integrar mecanismos técnicos de controlo de acesso e adaptação contextual no desenvolvimento de sistemas de informação, permitindo que os princípios de proteção de dados sejam efetivamente aplicados na arquitetura das soluções tecnológicas.

## 2.11. Privacidade no Contexto Computação Quântica: Desafios e perspetivas atuais

O avanço da computação quântica introduz uma nova variável no debate sobre segurança e privacidade. A capacidade de processamento exponencialmente superior pode, em determinados cenários, comprometer mecanismos criptográficos atualmente considerados seguros. Simultaneamente, a própria tecnologia quântica abre possibilidades de desenvolvimento de novos modelos de proteção, como técnicas avançadas de encriptação e modelos diferenciados de preservação de confidencialidade. A discussão permanece em evolução, exigindo reflexão contínua sobre impactos futuros na arquitetura de sistemas digitais (Michele Nogueira, 2025; Yalcin et al., 2024).

### 2.11.1. Ameaças à Privacidade Causados pela Computação Quântica

Complexidade e novas vulnerabilidades: modelos de computação que utilizam capacidades quânticas (como computação distribuída quântica) também podem enfrentar problemas de vazamento de privacidade semelhantes à computação clássica, exigindo mecanismos próprios para garantir confidencialidade em cenários quânticos (Zhong et al., 2025).

### 2.11.2. Oportunidade e Mecanismo Quânticos para Proteger a Privacidade

**Privacidade algorítmica quântica:** pesquisas recentes exploram como construir computação com preservação de privacidade, com base em tecnologia quântica, incluindo propostas de computação segura multipartidária, transferências obliviosa e criptografia homomórfica em ambientes quânticos. Essas abordagens podem permitir a análise de dados sensíveis sem revelar a informação subjacente (Gómez-Goiri et al., 2025).

**Modelos de privacidade diferencial quântica:** Novos conceitos emergentes, como a Quantum Differential Privacy ou extensões híbridas, buscam incorporar ruído quântico para proteger a privacidade, ao mesmo tempo em que minimizam a perda de utilidade dos dados processados em sistemas quânticos (Song et al., 2025).

## 2.12. Privacy by Design e Privacy by Default

A proteção de dados na perspectiva preventiva baseia-se na concepção de que a privacidade deve ser incorporada desde o início do desenvolvimento tecnológico, em vez de apenas corrigir falhas depois. Assim, as decisões arquitetónicas passam a refletir limites operacionais que restringem automaticamente a recolha excessiva de dados e configuram o sistema segundo a alternativa menos intrusiva Regulamento (UE) n.º 2016/679). Tal orientação desloca a conformidade do plano documental para o plano técnico operacional, reforçando a materialização prática dos princípios normativos.

## 2.13. Enquadramento Comparativo entre o Regime de Proteção de Dados de Cabo Verde e Portugal/UE

É importante destacar que a criação da legislação de privacidade e proteção de dados resulta da necessidade de proteger as informações diante de vários incidentes e ataques informáticos.

Atualmente, a proteção de dados pessoais é um elemento fundamental na política de governação digital, destacando a importância do direito à autodeterminação informativa nas sociedades modernas. Mesmo estando inseridos em enquadramentos normativos diferentes, os dois

regimes, tanto o cabo-verdiano como o português, revelam uma convergência em termos de princípios que norteiam a privacidade no espaço europeu e internacional.

Em Portugal, o tratamento de dados pessoais é praticamente regulado pelo Regulamento Geral sobre a Proteção de Dados (RGPD - 2016/679), um instrumento jurídico aplicado diretamente em todos os Estados da União Europeia. Este instrumento visa criar um modelo de harmonização normativa assente na responsabilização e na gestão de risco.

Em Cabo Verde, o quadro jurídico é definido pela Lei n.º 133/V/2001, que foi revista pela Lei n.º 41/VIII/2013 e alterada pela Lei n.º 121/IX/2021. A legislação cabo-verdiana é soberana, mas revela uma grande convergência conceptual com o modelo europeu. A supervisão e fiscalização ficam sob a responsabilidade da Comissão Nacional de Proteção de Dados de Cabo Verde, que desempenha um papel estratégico na promoção e sensibilização de uma cultura de proteção de informação. Mesmo com as semelhanças das duas entidades, existem diferenças na forma como atuam. A Comissão Nacional de Proteção de Dados de Cabo Verde (CNPD-CV) é mais voltado para a prevenção e, em determinados casos, é necessária uma autorização prévia, especialmente quando se trata de dados mais sensíveis. Por outro lado, a RGPD prioriza o modelo de responsabilização, atribuindo aos responsáveis a obrigação pelo tratamento e demostrar a conformidade com os princípios e normas de proteção.

No que diz respeito ao tratamento de dados pessoais, ambos os regimes concordam em vários princípios, como a licitude, a transparência e a lealdade na utilização de dados, a limitação na recolha mínima necessária de dados, os mesmos devem estar atualizados, restrição no tempo de conservação e a proteção para evitar acessos indevidos. Quanto aos direitos do titular, destacam-se o acesso, retificação, oposição, eliminação e, em termos análogos, portabilidade e revisão de decisões automatizadas, que encontram proteção em ambos os sistemas, ainda que com diferentes graus de densificação normativa. Embora existam semelhanças, ainda subsistem diferenças significativas no âmbito teórico e estrutural. O RGPD confere maior autonomia ao titular de dados e adota uma abordagem dinâmica, que envolve uma avaliação contínua dos riscos e a implementação de medidas técnicas e organizacionais proporcionais. Já, por sua vez, o regime cabo-verdiano, embora influenciado por essa lógica, mantém uma estrutura normativa mais formalista, que se baseia em procedimentos de autorização e em requisitos prévios mais claros, o que demonstra uma forma de regulação que foi ajustada a um contexto institucional distinto.

Em conclusão, a análise comparativa evidencia que os dois regimes partilham os mesmos valores base fundamentais, mas utilizam mecanismos diferentes para aplicar as regras e na distribuição de responsabilidades entre as entidades reguladas e as autoridades de supervisão.

Na abordagem teórica, Cabo Verde segue um modelo híbrido, situado entre o paradigma europeu de autorregulamentação supervisionada e um modelo mais tradicional de controlo normativo. Ainda assim mantém uma orientação inequívoca para a proteção forte dos direitos fundamentais no ambiente digital.

O protótipo proposto terá como finalidade proporcionar ao turista uma experiência segura e personalizada, permitindo o acesso a informações relativas a pontos turísticos, eventos locais e serviços complementares. Para que tal seja possível, torna-se necessário que os turistas se registem e forneçam dados pessoais.

Perante a necessidade da recolha de dados do turista, a concepção do protótipo baseia-se nos princípios do Regulamento Geral sobre a Proteção de Dados, aplicável a todas as entidades que tratem dados pessoais de cidadãos da União Europeia, e pelas boas práticas da Comissão Nacional de Proteção de Dados de Cabo Verde.

O tratamento de dados no protótipo respeita os princípios fundamentais estabelecidos no artigo 5.º do RGPD:

- Licitude, lealdade e transparência: o utilizador tem de estar informado de forma clara para sobre como os seus dados estão sendo recolhidos;
- Limitação das finalidades: os dados são recolhidos apenas para fins relacionados com o funcionamento da aplicação;
- Minimização dos dados: só devem ser recolhidos apenas os dados necessários, para que não haja recolhas desnecessárias;
- Exatidão: os utilizadores podem atualizar ou corrigir os seus dados através do perfil pessoal sempre que for necessário;
- Limitação da conservação: os dados são guardados apenas pelo período necessário para cumprir a finalidade para a qual foram recolhidos;
- Integridade e confidencialidade: garantir que os dados estejam seguros, atualizados e permitidos apenas para quem tem autorização;

### 2.13.1. Quadros Comparativos da Legislação Cabo-Verdiana e Portuguesa/EU

**Tabela 1 - Princípios fundamentais da proteção de dados**

| Dimensão | Legislação cabo-verdiana | RGPD (UE) |
|---|---|---|
| Licitude, lealdade e transparência | Tratamento baseado em fundamento legal e informação clara ao titular | Art.º 5.º, n.º 1, al. a) |

| | | |
|---|---|---|
| Limitação da finalidade | Dados recolhidos para finalidades determinadas e legítimas | Art.º 5.º, n.º 1, al. b) |
| Minimização dos dados | Recolha limitada ao estritamente necessário | Art.º 5.º, n. º 1, al. c) |
| Exatidão | Dados exato e atualizados | Art.º 5.º, n.º 1, al. d) |
| Limitação da conservação | Conservação apenas pelo período necessário | Art.º 5.º, n.º 1, al. e) |
| Integridade e confidencialidade | Medidas técnicas e organizativas adequadas | Art.º 5.º, n.º 1, al. f) |

**Tabela 2 - Direitos dos titulares dos dados**

| Direito | Cabo Verde | RGPD (UE) |
|---|---|---|
| Direito à informação | Artº 13 | Art.º 13.º e 14.º |
| Direito de acesso | Artº 14 | Art.º 15.º |
| Direito de retificação | Artº 15 | Art.º 16.º |
| Direito ao apagamento | Artº 16 | Art.º 17.º |
| Direito à limitação do tratamento | Artº 17 | Art.º 18.º |
| Direito de objeção | Artº 20 | Art.º 21.º |
| Direito à portabilidade | Artº 18 | Art.º 20.º |

**Tabela 3 - Obrigações das entidades responsáveis pelo tratamento**

| Obrigação | Cabo Verde | RGPD (UE) |
|---|---|---|
| Base legal para o tratamento | Obrigatória | Art.º 6.º |
| Consentimento explícito | Exigido em determinados casos | Art.º 7.º |
| Medidas de segurança | Obrigatória | Art.º 32.º |
| Registo das atividades de tratamento | Recomendado | Art.º 30.º |
| Notificação de violações de dados | Obrigatória | Art.º 33.º e 34.º |
| Avaliação de impacto | Prevista para casos de risco elevado | Art.º 35.º |

**Tabela 4 - Privacy by design e Privacy by default**

| Aspecto | Cabo Verde | RGPD (UE) |
|---|---|---|
| Integração da privacidade desde a concepção | Implícita no regime legal | Art.º 25.º |
| Configurações por defeito | Incentivadas | Art.º 25.º, n.º 2 |
| Responsabilização do responsável | Prevista | Art.º 5.º, n.º 2 |

**Tabela 5 - Relevância para o sector do turismo**

| Dimensão | Implicações Práticas |
|---|---|
| Recolha de dados | Limitação a dados estritamente necessários para os serviços |
| Partilha de dados | Contratos claros com operadores e plataformas |
| Segurança | Proteção reforçada de dados de pagamento e identificação |
| Transparência | Políticas de privacidade claras e acessíveis |

# CAPÍTULO 3

# Metodologia de Investigação

## 3.1 Abordagem Metodológica

Para o desenvolvimento desta pesquisa, adotar-se-á a metodologia Design Science Research. O Design Science Research é uma metodologia com dupla visão. Por um lado, tem como objetivo o desenvolvimento e avaliação de artefactos com a finalidade de resolver um problema específico e, por outro, a geração de conhecimento científico (Madureira & Schneider, 2025). O DSR é pertencente as ciências exatas, mas concretamente à ciência da computação, mas é transversal à área de conhecimento ou de pesquisa. A Design Science Research estrutura-se em seis fases principais que norteiam o desenvolvimento desta investigação (Elizabete et al., 2022).

**Tabela 6 - Processo metodológico baseado em Design Science Research**

| **Metodologia Design Science Research** | |
|---|---|
| **Fases** | **Descrição** |
| Problema de Investigação | Nesta etapa da investigação, consiste na análise do contexto turístico e desafios na gestão de dados. |
| Definir os requisitos da Solução | Com base no problema identificado, procede-se ao levantamento dos requisitos funcionais e não funcionais da plataforma digital. |
| Desenvolvimento do Artefacto | Concepção da arquitetura e implementação da plataforma digital. |
| Demonstração do Artefacto | Após o desenvolvimento do protótipo, é apresentado aos utilizadores. |
| Avaliação do Artefacto | A etapa de avaliação tem como objetivo analisar a plataforma com base em critérios como eficácia, eficiência, utilidade e relevância para o contexto organizacional. |
| Comunicação dos Resultados | Comunicação dos resultados, divulgação científica e contributos do estudo. |

## 3.2 Ciclos da Design Science Research

A metodologia DSR organiza-se em três ciclos interligados: o Ciclo de Relevância, o Ciclo Empírico (Rigor) e o Ciclo de Engenharia (Design), conforme ilustrado na figura 4 (Hevner, 2007).

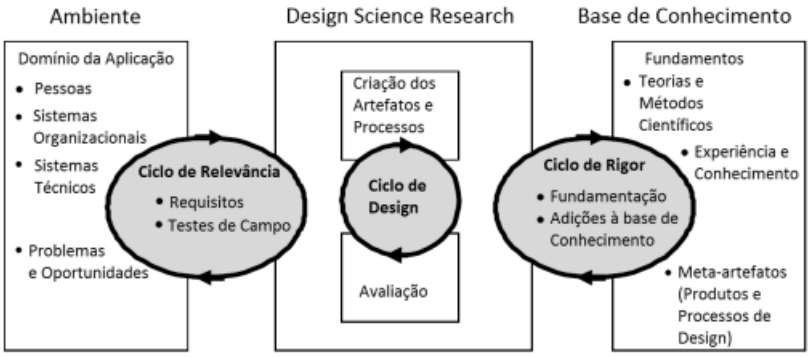



***Figura 4 - Ciclo DSR***

### 3.2.1 Ciclo de Relevância

O Ciclo de Relevância relaciona-se entre a investigação e a identificação do problema no contexto real. Neste sentido, neste ciclo, fez-se a análise e levantamento de requisitos, identificação dos stakeholders e, em particular, das atuais práticas executadas no tratamento de dados pessoais e nos desafios associados à privacidade e proteção de dados (Hevner, 2007).

### 3.2.2 Ciclo de Rigor

O Ciclo Empírico (do Rigor) assegura que a investigação se baseia em métodos científicos consolidado. Neste contexto, recorre-se à revisão da literatura, à análise da legislação cabo-verdiana sobre proteção de dados pessoais e aos enquadramentos normativos internacionais aplicáveis, nomeadamente o Regulamento Geral sobre a Proteção de Dados, como pode-se ver na figura 5 algumas atividades a serem realizadas nesse ciclo (Pimentel et al., 2018).




***Figura 5 - Ciclo empírico***

### 3.2.3 Ciclo de Engenharia

No Ciclo de Engenharia (Design), realiza-se o desenvolvimento e a avaliação do artefacto. Nesta fase define-se a arquitetura da aplicação, integrando os princípios de privacidade e na

avaliação da solução. Na figura 6, estão listadas algumas atividades a serem realizadas (Pimentel et al., 2018).




***Figura 6 - Ciclo de engenharia***

### 3.3 Métodos de Recolha de Dados

Considerando os objetivos do estudo e o seu carácter aplicado e exploratório, utilizou-se uma abordagem qualitativa e documental. Desde forma, foi possível uma análise aprofundada do fenómeno em estudo, recorrendo a diversas fontes de informação, conforme sugerido na literatura da área dos Sistemas de Informação (Myers, 2020).

A investigação focou-se na análise documental e na realização de questionário. No que concerne à análise documental, foram examinados os documentos oficiais cabo-verdianos e internacionais relacionados com privacidade e proteção de dados pessoais, bem como normas técnicas e estudos científicos recentes. Esta etapa permitiu enquadrar o problema de investigação e identificar os principais requisitos legais e normativos relevantes (Bowen, 2009).

Sempre que foi possível, fez-se a observação direta de processos e sistemas utilizados no sector do turismo, permitindo identificar o modo como os dados pessoais são tratados e os riscos associados a esse tratamento.

### 3.4 Critérios de Avaliação do Artefacto

A avaliação do artefacto é a etapa fundamental na Design Science Research, pois permite verificar se o artefacto desenvolvido gerou valor perante o problema identificado no contexto do setor do turismo. Neste âmbito, procurou-se validar se o artefacto estava dentro da legislação e princípios de proteção de dados de acordo com as normas cabo-verdianas e internacionais. Adicionalmente, avaliou-se a sua usabilidade por diferentes tipos de usuários, bem como a satisfação e confiança da plataforma digital pelos usuários.

Este critério baseia-se nas recomendações metodológicas da Design Science Research, que destacam a necessidade de métricas claras e objetivas para avaliar o desempenho do artefacto (Hevner et al., 2004).

# CAPÍTULO 4

# Análise e a Identificação dos Requisitos

## 4.1 Identificação de Stakeholders

A identificação dos stakeholders é importante no processo de levantamento dos requisitos, permitindo compreender as necessidades, responsabilidades e expectativas dos diferentes intervenientes envolvidos no ecossistema turístico. A plataforma digital proposta tem vários stakeholders que interagem com o sistema direta ou indiretamente no tratamento e gestão de dados pessoais.

Para garantir uma gestão ética e segura da informação, torna-se fundamental definir os níveis de acesso dos diferentes perfis que acedem à plataforma. Além do perfil do turista, que é o principal utilizador do sistema, devem também ser considerados outros perfis institucionais, como operadores turísticos, prestadores de serviços e entidades públicas responsáveis pela regulação e supervisão do setor.

A participação ativa do utilizador no processo de registo e fornecimento de dados assume particular importância no funcionamento da plataforma digital. A disponibilização voluntária de informações básicas de identificação permite uma personalização dos serviços turísticos e contribui para uma experiência digital mais adequada às preferências do utilizador. De acordo com (Reis Quietinho Leithardt et al., 2013), o utilizador tem a possibilidade de autorizar o acesso às suas informações e aos serviços associados, permitindo não apenas uma utilização mais eficiente da plataforma, mas também contribuindo para o aprimoramento contínuo do sistema.

Adicionalmente, a definição de um mecanismo estruturante hierarquicamente de utilizadores revela-se essencial para assegurar uma gestão correta dos níveis de acesso e das permissões associadas a cada perfil. Esta abordagem permite estabelecer diferentes níveis de autorização no sistema, assegurando que cada utilizador interage com a plataforma de acordo com o seu nível de perfil e funções específicas. A adoção de modelos de controlo de acesso baseados em papéis contribui para reforçar a segurança da informação, reduzir riscos de acesso indevido e assegurar o cumprimento dos princípios normativos e de proteção de informação

domínio, sendo, por isso, pertinente apresentar uma visão geral dessas legislações e da forma como regulam o tratamento de dados pessoais.

## 4.2 Levantamento de Requisitos Funcionais / Requisitos Não Funcionais

Com base na análise do contexto e na identificação de Stakeholders, abaixo segue as tabelas com os requisitos funcionais e não funcionais essenciais da plataforma:

**Tabela 7 - Requisitos funcionais e Comportamento esperado do sistema**

| ID | Requisito Funcional | Descrição | Comportamento Esperado |
|---|---|---|---|
| RF01 | Registo/Autenticação | O sistema deve permitir criar conta e autenticar o acesso. | O sistema deve validar o user e a palavra-passe e ativar autenticação multifator (MFA). Caso os dados de login estejam incorretos, o sistema deve bloquear o acesso. |
| RF02 | Gestão de Perfis de Utilizador | Permitir consulta e a atualização de dados pessoais do utilizador. | O sistema deve permitir ao utilizador visualizar, editar e atualizar os seus dados pessoais em tempo real, garantindo rastreabilidade das alterações. |
| RF03 | Pesquisa e Reserva de Serviços Turísticos | Consulta de serviços e realização de reservas. | O sistema deve permitir pesquisa por filtros dos serviços disponibilizados e confirmar a reserva apenas após validação dos dados estritamente necessários. |
| RF04 | Gestão de Consentimento | Recolha e registo do consentimento. | O sistema deve recolher consentimento explícito, granular e separado para cada finalidade de tratamento, armazenando prova digital. |
| RF05 | Gestão de Direitos do Titular | Exercício de direitos (acesso, retificação, apagamento, limitação). | O sistema deve ter uma opção de interface para que os usuários possam submeter o pedido automático e resposta dentro do prazo legal estabelecido. |
| RF06 | Sistema de Notificação de Incidentes | Gestão de Violações de dados. | O sistema deve registar qualquer tipo de incidentes ocorrido fora da normalidade e permitir uma comunicação à entidade responsável, quando aplicável. |
| RF07 | Painel Administrativo com Controlo de Acessos | Gestão interna da plataforma. | O sistema deve aplicar o princípio do menor privilégio, diferenciando perfis. |

**Tabela 8 - Requisitos não funcionais**

| ID | Requisito Não Funcional | Descrição |
|---|---|---|
| RNF01 | Segurança | O sistema deve garantir mecanismos de autenticação e controlo de acessos para evitar acessos não autorizados aos dados. |
| RNF02 | Privacidade | O sistema deve assegurar que apenas os dados estritamente necessários são recolhidos e tratados, de acordo com o princípio da minimização de dados. Este requisito está diretamente alinhado com os princípios de Privacy by Design e Privacy by Default. |
| RNF03 | Usabilidade | A interface do sistema deve ser intuitiva e facilitar a interação do utilizador com a aplicação. Adicionalmente, o sistema deve permitir que os utilizadores compreendam de forma clara como os dados são recolhidos e utilizados. |
| RNF04 | Escalabilidade | A arquitetura do sistema deve permitir a evolução futura da aplicação, possibilitando a integração de novas funcionalidades ou a adaptação a diferentes contextos organizacionais. |
| RNF05 | Fiabilidade | O sistema deve garantir a integridade e consistência dos dados armazenados, prevenindo alterações não autorizadas e assegurando a fiabilidade da informação. |

## 4.3 Requisitos de Privacidade e Proteção de Dados

A plataforma digital proposta cumpre os requisitos legais, técnicos e organizacionais, assegurando uma abordagem integrada à proteção de dados. Este enquadramento normativo, que é regulamentado pela Lei nº 121/IX/2021, com a supervisão da Comissão Nacional de Proteção de dados de Cabo Verde, bem como as normas internacionais consagradas no Regulamento Geral de Proteção de Dados da União Europeia n.º 2016/679, assegura que a plataforma cumpra os princípios de Privacy by Design e Privacy by Default.

### 4.3.1 Requisitos da base legal aplicável

**Licitude, lealdade e transparência no tratamento de dados:** o tratamento de dados pessoais deve estar baseado na norma jurídica válida, como o consentimento do titular, a execução de contrato. No protótipo proposto, a licitude dos tratamentos de dados pessoais é assegurada mediante a recolha de consentimento claro e específico para cada objetivo definido. O titular de dados deve ter informação clara sobre os objetivos do tratamento, desta forma criando um ambiente de confiança. O que garanta o processamento ocorra de acordo com os critérios legais e não de maneira arbitrária ou abusiva.

**Minimização da recolha de dados:** o protótipo deverá recolher apenas os dados estritamente necessários para a finalidade desejada. Garantindo a limitação de campos obrigatórios no formulário, assim evitando recolhas de dados sensíveis sem necessidade. É

muito pertinente uma revisão periódica das informações armazenadas; assim, reduz exposição de dados indevidos.

**Garantia dos direitos dos titulares:** os titulares devem ter a garantia de exercer em pleno os seus direitos de acessos dos seus dados pessoais, retificação de informações, apagamento de dados e limitação do tratamento.

**Implementação de medidas adequadas de segurança:** o responsável pelo tratamento deve assegurar que as soluções implementadas sejam proporcionais aos riscos associados no tratamento de dados. Ter um controlo de acesso eficaz, e uma política de aplicação de normas internas de segurança e uma proteção de informação através de encriptação.

**Responsabilidade demonstrável:** o responsável pelo tratamento de dados não adianta que cumpra as leis ou as suas obrigações legais. Há necessidade de comprovar de forma clara e documental. Para que isso seja possível, é necessário que guarde as provas dos registos das atividades realizadas e os consentimentos obtidos. O que reforça a transparência e confiança dos stakeholders.

### 4.3.2 Requisitos técnicos

**Encriptação de dados em trânsito e em repouso**: os dados devem ser protegidos com encriptação tanto quando são enviados como quando são guardados. Para o envio, usam-se protocolos seguros, como o TLS 1.2, para que a informação não seja intercetada. Para o armazenamento, a base de dados é encriptada, impedindo o acesso por pessoas não autorizadas e reduzindo o risco de violação da privacidade.

**Autenticação multifator:** uma autenticação forte reduz o risco de acesso não autorizado, usando uma palavra-passe robustas, a implementação de autenticação multifator e um bloqueio automático após sucessivas tentativas falhadas.

**Sistema de Gestão de incidentes**: o sistema deve ter capacidade de detetar atividades suspeitas e ter registo formal e estruturado de todos os incidentes acontecidos, e uma política de resposta de comunicação que abranja as entidades competentes, com o objetivo de ter uma ação eficaz e rápida perante situações que possam comprometer a segurança dos dados.

**Registo de atividades de tratamento**: a plataforma deve ser capaz de rastrear as atividades, através da data e hora, qual usuário as realizou e que tipo de operação fez no sistema. Assim, desta forma, com este mecanismo estratégico, é possível ter o controlo interno e apuração de responsabilidade em caso de incidentes de uso arbitrário.

### 4.3.3 Requisitos organizacionais

A implementação da solução tecnológica exige a definição de mecanismos organizacionais que assegurem controlo, responsabilidade e conformidade no tratamento de dados. Para além dos requisitos técnicos, a eficácia do sistema depende de práticas internas estruturadas, alinhadas com princípios de governação, mitigação de riscos e proteção da informação.

**Definição clara de responsabilidades internas:** a organização deve estabelecer uma clara delimitação de funções entre os vários tipos de perfis envolvidos na operação da plataforma. Como os administradores, operadores funcionais e a entidade responsável pela supervisão da proteção de dados. A separação de responsabilidades constitui um mecanismo essencial de controlo interno, reduzindo conflitos de competências e limitando a possibilidade de acessos indevidos. Esta distinção funcional contribui para maior rastreabilidade das ações realizadas no sistema e reforça a responsabilização individual no âmbito do tratamento de dados.

**Formação dos colaboradores em proteção de dados:** a consolidação de uma cultura organizacional orientada para a segurança da informação depende da formação sistemática dos colaboradores. A capacitação contínua permite ampliar o conhecimento relativo às obrigações legais aplicáveis, promover práticas responsáveis no tratamento de dados e reduzir vulnerabilidades associadas ao fator humano. Evidências recentes apontam que a componente humana permanece como um dos principais vetores de incidentes de segurança, o que reforça a necessidade de investimento permanente em sensibilização e qualificação interna (ENISA, 2024).

**Procedimentos internos de resposta a incidentes:** a organização deve dispor de um modelo documentado para tratamento de incidentes relacionados com segurança da informação e proteção de dados. Tal modelo deve especificar:

- Os mecanismos de deteção, registo e classificação do incidente;
- Os níveis de reporte e critérios de escalonamento interno;
- Os procedimentos de comunicação com entidades externas e partes interessadas;
- As medidas corretivas e preventivas destinadas à mitigação de impactos e prevenção de recorrências.

A formalização destes procedimentos reduz a improvisação em contextos críticos, assegura consistência na resposta organizacional e demonstra diligência no cumprimento das obrigações legais e regulamentares.

**Realização de avaliações de impacto quando necessário:** sempre que o tratamento de dados apresentar elevado risco para os titulares, devem ser realizadas avaliações de impacto

adequadas. A integração deste mecanismo desde a fase de concepção da solução reforça uma abordagem preventiva, permitindo identificar vulnerabilidades antes da entrada em produção e implementar salvaguardas proporcionais aos riscos identificados.

## 4.4 Diagramas de Casos de Uso

Os casos de uso constituem uma ferramenta fundamental para a representação e compreensão das funcionalidades de uma plataforma digital. Com isso, é possível descrever de forma clara a interação de todos os intervenientes com o sistema e quais são as ações que cada um poderá realizar. Essa abordagem facilita a identificação dos requisitos funcionais, permitindo visualizar os processos e as operações que o sistema deve suportar para atender às necessidades dos utilizadores.

A figura 7 ilustra o diagrama de caso de uso com a visão global do sistema, com as interações entre os atores e o sistema de serviços turísticos, evidenciando as principais funcionalidades com foco no mecanismo de proteção de dados e salvaguarda da privacidade dos utilizadores.

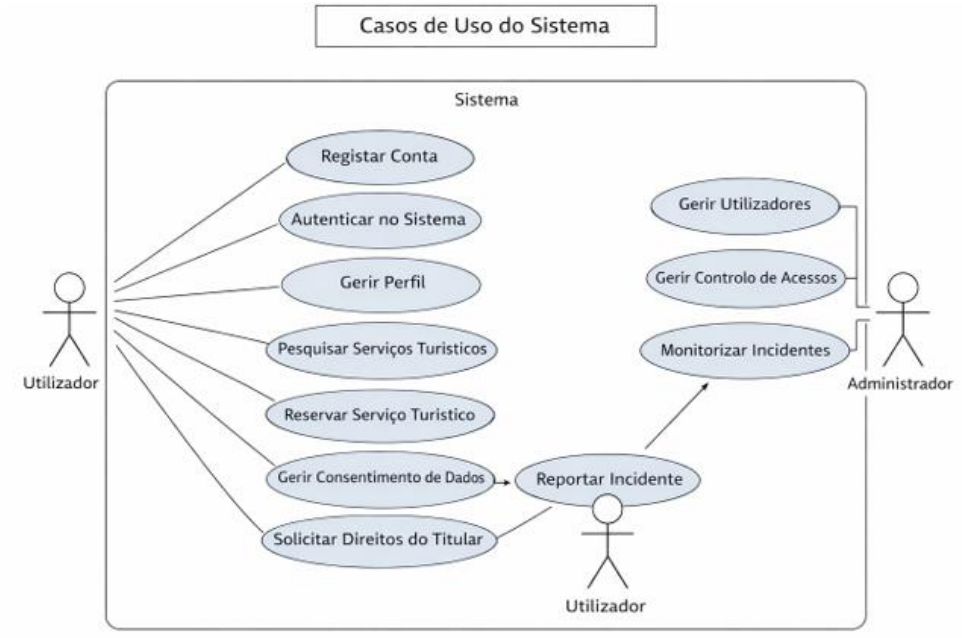



***Figura 7 - Interação dos atores com o sistema na Visão Global***

### 4.4.1 Descrição de Caso de Uso

Nesta seção são descritos os casos de uso identificados para a plataforma digital. Cada caso de uso representa uma interação entre o interveniente e o sistema e permite compreender de que

forma as funcionalidades disponíveis são utilizadas no contexto da aplicação. A descrição destes elementos possibilita uma visão estruturada das operações que podem ser realizadas, bem como das funcionalidades às quais cada utilizador terá acesso.

**Tabela 9 - Caso de uso de Registo de utilizador**

| **Nome** | **Registo de Utilizador** |
|---|---|
| Ator principal | Turista |
| Descrição | Permite ao utilizador criar uma conta na plataforma de forma segura. |
| Pré-condições | O utilizador não possui conta registada na plataforma. |
| Cenário principal | 1. O utilizador seleciona a opção de registo.<br>2. O utilizador introduz dados pessoais obrigatórios.<br>3. O utilizador aceita os termos e condições.<br>4. A plataforma valida os dados introduzidos.<br>5. A plataforma solicita verificação adicional.<br>6. O utilizador insere o código de verificação adicional.<br>7. A plataforma cria a conta. |
| Cenário alternativo | 1. A1: conta já existente.<br>• A plataforma apresenta mensagem de erro.<br>• O utilizador deve inserir outro email.<br>2. A2: dados inválidos ou incompletos.<br>• A plataforma apresenta mensagem de erro.<br>• O utilizador deve corrigir os dados. |
| Pós-condições | Conta criada com sucesso e utilizador autenticado na plataforma. |

**Tabela 10 - Caso de uso de Autenticação de utilizador**

| **Nome** | **Autenticação de Utilizador** |
|---|---|
| Ator principal | Turista |
| Descrição | Permite que um utilizador registado aceda à plataforma através da sua conta criada. |
| Pré-condição | O utilizador ter uma conta válida na plataforma. |
| Cenário principal | 1. O utilizador acede à página de login.<br>2. O utilizador introduz as suas credenciais (e-mail e palavra-passe).<br>3. A plataforma valida as credenciais introduzidas.<br>4. A plataforma autentica o utilizador.<br>5. O utilizador terá acesso à plataforma. |
| Cenário alternativo | 1. A1: credencias inválidas.<br>• A plataforma detecta credenciais inválidas.<br>• A plataforma apresenta mensagem de erro.<br>• O utilizador tenta novamente.<br>2. A2: conta bloqueada.<br>• A plataforma informa que conta está bloqueada.<br>• O utilizador entra em contato com suporte. |
| Pós-condições | O utilizador autenticado e com acesso às funcionalidades da plataforma. |

**Tabela 11 - Caso de uso de Gestão de perfil de utilizador**

| **Nome** | **Gestão de Perfil de Utilizador** |
|---|---|
| Ator principal | Turista |
| Descrição | Permite ao utilizador visualizar e atualizar as suas informações pessoais. |
| Pré-condição | O utilizador autenticado na plataforma. |
| Cenário principal | 1. O utilizador acede à área de perfil.<br>2. A plataforma apresenta as informações pessoais registado.<br>3. O utilizador edita os dados pessoais desejados.<br>4. O utilizador submete as alterações realizadas.<br>5. A plataforma valida os dados introduzidos.<br>6. O sistema guarda as alterações realizadas.<br>7. A plataforma confirma a atualização ao utilizador. |
| Cenário alternativo | 1. A1: dados inválidos.<br>• O sistema detecta dados inválidos.<br>• O sistema apresenta mensagem de erro.<br>• O utilizador corrige os dados e tenta novamente.<br>2. A2: cancelamento da operação.<br>• O utilizador cancela a edição.<br>• O sistema mantém os dados originais.<br>3. A3: erro ao guardar na plataforma.<br>• O sistema falha ao guardar os dados.<br>• O sistema informa o utilizador do erro. |
| Pós-condições | Os dados do utilizador são atualizados com sucesso na plataforma. |

**Tabela 12 - Caso de uso de Pesquisa de serviços turísticos**

| **Nome** | **Pesquisa de Serviços Turísticos** |
|---|---|
| Ator principal | Turista |
| Descrição | Permite ao utilizador pesquisar serviços turísticos disponíveis na plataforma. |
| Pré-condição | O utilizador autenticado na plataforma. |
| Cenário principal | 1. O utilizador acede à funcionalidade de pesquisa.<br>2. O utilizador introduz os filtros de pesquisa.<br>3. A plataforma processa os critérios da pesquisa.<br>4. A plataforma apresenta a lista de serviços turísticos disponíveis. |
| Cenário alternativo | 1. A1: sem resultados.<br>• A plataforma não encontra serviços correspondentes aos critérios.<br>• A plataforma informa o utilizador de que não existem resultados.<br>2. A2: erro na plataforma.<br>• Ocorre uma falha no processamento da pesquisa.<br>• A plataforma informa o utilizador do erro. |
| Pós-condições | Os resultados da pesquisa são apresentados ao utilizador. |

**Tabela 13 - Caso de uso de Reservar serviço turístico**

| Nome | Reservar Serviço Turístico |
|---|---|
| Ator principal | Turista |
| Descrição | Permite ao utilizador reservar um serviço turístico disponível. |
| Pré-condição | O utilizador autenticado na plataforma. |
| Cenário principal | 1. O utilizador seleciona um serviço turístico desejado.<br>2. A plataforma apresenta os detalhes do serviço selecionado.<br>3. O utilizador confirma a reserva.<br>4. A plataforma regista a reserva.<br>5. A plataforma envia confirmação ao utilizador. |
| Cenário alternativo | 1. A1: serviço indisponível.<br>• A plataforma detecta que o serviço não está disponível.<br>• A plataforma informa o utilizador.<br>2. A2: cancelamento da reserva.<br>• O utilizador cancela o processo de reserva.<br>• A plataforma não regista qualquer reserva.<br>3. A3: erro na plataforma.<br>• Ocorre uma falha ao registar a reserva.<br>• A plataforma informa o utilizador do erro. |
| Pós-condições | A reserva é registada na plataforma.<br>O utilizador recebe confirmação da reserva. |

**Tabela 14 - Caso de uso de Gestão de consentimento**

| Nome | Gestão de Consentimento |
|---|---|
| Ator principal | Turista |
| Descrição | Permitir ao utilizador autorizar, recusar ou retirar o consentimento para o tratamento dos seus dados pessoais, de acordo com diferentes finalidades. |
| Pré-condição | O utilizador autenticado na plataforma. |
| Cenário principal | 1. O utilizador acede à área de gestão de consentimento.<br>2. A plataforma apresenta as finalidades de tratamento de dados.<br>3. O utilizador seleciona as opções de consentimento.<br>4. O utilizador confirma a sua decisão.<br>5. A plataforma regista decisão com data e hora.<br>6. A plataforma atualiza o estado de consentimento do utilizador. |
| Cenário alternativo | 1. A1: erro no registo.<br>• A plataforma falha ao registar o consentimento.<br>• A plataforma informa o utilizador do erro.<br>2. A2: cancelamento da operação.<br>• O utilizador sai da página sem confirmar.<br>• A plataforma não altera o estado do consentimento. |
| Pós-condições | O consentimento do utilizador é atualizado no sistema.<br>O registo é armazenado para fins de auditoria e conformidade legal. |

**Tabela 15 - Caso de uso de Gestão de direitos do titular**

| Nome | Gestão de Direitos do Titular |
|---|---|
| Ator principal | Turista |
| Ator secundário | Administrador |
| Descrição | Permite ao utilizador exercer os seus direitos de dados pessoais, incluindo acesso, retificação, apagamento, portabilidade e recusa de tratamento dos dados. |
| Pré-condição | O utilizador autenticado na plataforma. |
| | 1. O utilizador acede à área de direitos do titular.<br>2. A plataforma disponibiliza os direitos disponíveis.<br>3. O utilizador seleciona o direito pretendido.<br>4. O utilizador submete o pedido.<br>5. A plataforma valida e regista o pedido.<br>6. A plataforma notifica o administrador.<br>7. Administrador analisa e processa o pedido.<br>8. A plataforma informa o utilizador sobre o estado ou resultado do pedido. |
| Cenário alternativo | 1. A1: pedido inválido.<br>• A plataforma detecta informação incompleta ou inválida.<br>• A plataforma solicita correção ao utilizador.<br>2. A2: rejeição do pedido.<br>• O administrador rejeita o pedido.<br>• A plataforma informa o utilizador com justificação.<br>3. A3: erro no sistema.<br>• Ocorre uma falha no registo ou processamento do pedido.<br>• A plataforma informa o utilizador.<br>4. A4: cancelamento pelo utilizador.<br>• O utilizador cancela o pedido antes do envio.<br>• A plataforma não regista o pedido. |
| Pós-condições | O pedido do utilizador é registado e processado.<br>O sistema mantém registo para auditoria e conformidade legal.<br>O utilizador é informado sobre o resultado do pedido. |

**Tabela 16 - Caso de uso Reportar incidente**

| Nome | Reportar Incidente |
|---|---|
| Ator principal | Turista |
| Ator secundário | Administrador |
| Descrição | Permite ao utilizador reportar incidentes relacionados com a segurança, funcionamento ou utilização da plataforma. |
| Pré-condição | O utilizador autenticado na plataforma. |
| Cenário principal | 1. O utilizador identifica um incidente.<br>2. O utilizador acede à área de reporte de incidentes.<br>3. A plataforma apresenta o formulário de reporte.<br>4. O utilizador introduz descrição do incidente.<br>5. O utilizador submete o reporte.<br>6. A plataforma valida a informação.<br>7. A plataforma regista o incidente.<br>8. A plataforma notifica os administradores.<br>9. A plataforma confirma o envio ao utilizador. |
| Cenário alternativo | 1. A1: dados incompletos.<br>• A plataforma detecta informação obrigatória em falta.<br>• A plataforma solicita correção ao utilizador.<br>2. A2: erro no registo.<br>• Ocorre uma falha ao registar o incidente.<br>• A plataforma informa o utilizador do erro. |

| | |
|---|---|
| | 3. A3: cancelamento.<br>• O utilizador cancela o reporte antes de submeter.<br>• A plataforma não regista o incidente. |
| Pós-condições | O incidente é registado no sistema.<br>O administrador é notificado.<br>O reporte fica disponível para análise e tratamento. |

**Tabela 17 - Caso de uso de Gestão de utilizadores**

| **Nome** | **Gestão de utilizadores** |
|---|---|
| Ator principal | Administrador |
| Descrição | Permite ao administrador visualizar, editar, ativar, desativar e gerir permissões dos utilizadores da plataforma. |
| Pré-condição | Administrador autenticado na plataforma. |
| Cenário principal | 1. Administrador acede ao painel administrativo.<br>2. A plataforma apresenta a lista de utilizadores.<br>3. O administrador seleciona um utilizador em causa.<br>4. A plataforma apresenta os detalhes do utilizador.<br>5. O administrador realiza ações de gestão que pretende.<br>6. O administrador confirma as alterações.<br>7. A plataforma valida e aplica as alterações.<br>8. A plataforma atualiza os dados do utilizador.<br>9. A plataforma confirma a operação ao administrador. |
| Cenário alternativo | 1. A1: o utilizador não encontrado.<br>• A plataforma não localiza o utilizador.<br>• A plataforma informa o administrador.<br>2. A2: erro na atualização.<br>• A plataforma falha ao aplicar alterações.<br>• A plataforma informa o administrador.<br>3. A3: ação não autorizada.<br>• O administrador tenta realizar uma ação sem permissão suficiente.<br>• A plataforma bloqueia a ação e apresenta mensagem de erro.<br>4. A4: cancelamento da operação.<br>• O administrador cancela a ação antes de confirmar.<br>• A plataforma não aplica alterações. |
| Pós-condições | Os dados do utilizador são atualizados na plataforma.<br>As alterações ficam registadas para auditoria. |

**Tabela 18 - Caso de uso de Gestão de perfil e controlo de acesso**

| **Nome** | **Gestão de Perfis e o controlo de Acesso** |
|---|---|
| Ator principal | Administrador |
| Descrição | Permite ao administrador definir permissões e níveis de acesso no sistema. |
| Pré-condição | Administrador autenticado na plataforma. |
| Cenário principal | 1. O administrador acede ao painel administrativo da plataforma.<br>2. A plataforma apresenta os perfis de acesso existentes.<br>3. O administrador cria ou seleciona um perfil.<br>4. A plataforma apresenta as permissões disponíveis. |

| | |
|---|---|
| | 5. O administrador define ou altera as permissões associadas ao perfil.<br>6. O administrador confirma as alterações.<br>7. A plataforma valida as configurações.<br>8. A plataforma aplica e guarda as permissões.<br>9. A plataforma confirma a operação ao administrador. |
| Cenário alternativo | 1. A1: conflito de permissões.<br>• A plataforma detecta configurações inconsistentes.<br>• A plataforma informa o administrador e solicita correção.<br>2. A2: erro ao guardar.<br>• A plataforma falha ao aplicar as permissões.<br>• A plataforma informa o administrador.<br>3. A3: ação inválida.<br>• O administrador tenta definir permissões não permitidas.<br>• A plataforma bloqueia a ação.<br>4. A4: cancelamento.<br>• O administrador cancela a operação antes de confirmar.<br>• A plataforma não aplica alterações. |
| Pós-condições | Os perfis e permissões são atualizados na plataforma.<br>As configurações ficam registadas para auditoria e controlo de acessos. |

**Tabela 19 - Caso de uso Monitorizar incidentes**

| **Nome** | **Monitorização de Incidentes** |
|---|---|
| Ator principal | Administrador |
| Descrição | Permite ao administrador visualizar, analisar, acompanhar e atualizar o estado dos incidentes reportados na plataforma. |
| Pré-condição | Administrador autenticado na plataforma. |
| Cenário principal | 1. O administrador acede à área de incidentes.<br>2. A plataforma apresenta lista de incidentes reportados.<br>3. O administrador seleciona um incidente.<br>4. A plataforma apresenta os detalhes do incidente.<br>5. O administrador analisa e atualiza o estado do incidente.<br>6. A plataforma guarda as atualizações.<br>7. A plataforma confirma a operação. |
| Cenário alternativo | 1. A1: incidente não encontrado.<br>• A plataforma não localiza o incidente.<br>• A plataforma informa o administrador.<br>2. A2: erro ao atualizar.<br>• A plataforma falha ao guardar alterações.<br>• A plataforma informa o administrador.<br>3. A3: atualização inválida.<br>• O administrador tenta definir um estado inválido.<br>• A plataforma bloqueia a ação e apresenta mensagem. |
| Pós-condições | O estado do incidente é atualizado na plataforma.<br>As ações realizadas ficam registadas para auditoria.<br>O incidente permanece disponível para acompanhamento. |

# CAPÍTULO 5

# Concepção e desenvolvimento do Protótipo

## 5.1 Introdução ao Protótipo

O capítulo anterior centrou-se no levantamento e na análise dos requisitos, bem como na definição dos casos de uso que serviram de base ao desenvolvimento do protótipo, concebido especificamente para o contexto do turismo cabo-verdiano e fundamentado nos referenciais normativos da CNPD-CV e RGPD.

Na sequência do trabalho desenvolvido, e considerando que a metodologia Design Science Research exige não apenas a proposição de um artefacto, mas também a sua demonstração e avaliação (Peffers et al., 2007), este capítulo avança da fase de conceção para a sua concretização prática.

A ideia geral do protótipo consiste na implementação de uma plataforma digital orientada para o turismo, incorporando os princípios de proteção de dados estabelecidos pelo CNPD-CV e RGPD. O protótipo visa apoiar os decisores e as organizações que operam na indústria do turismo na gestão estruturada e jurídica conforme é o ciclo de vida dos dados pessoais.

Esta abordagem justifica-se pela crescente digitalização do setor do turismo, que intensifica a utilização de sistemas de informação e torna fundamental a integração de requisitos normativos e legais desde as fases iniciais de conceção e desenvolvimento.

## 5.2 Arquitectura do Protótipo

A arquitectura proposta segue um modelo em camadas. Concebido para articular requisitos técnicos, exigências jurídicas e mecanismos de governação organizacional. Neste contexto, esta abordagem permite segmentar responsabilidades funcionais, reduzir dependências excessivas entre componentes e assegurar que os princípios de proteção de dados são operacionalizados de forma consistente ao longo do sistema.

### 5.2.1 Desenho da Interface do Utilizador

A interface do utilizador, ou popularmente conhecida como frontend, concentra os mecanismos de comunicação entre o sistema e os diferentes perfis organizacionais. A plataforma distingue níveis de utilização associados a funções específicas: administração

técnica, operação funcional e supervisão da proteção de dados, estabelecendo uma correspondência direta entre perfil e conjunto de permissões atribuídas.

O modelo de autorização implementado baseia-se numa lógica de atribuição de privilégios por função de controlo de Acesso Baseado em Papéis (RBAC), permitindo que o acesso às funcionalidades seja condicionado à responsabilidade efetivamente exercida. Esta política reduz a exposição desnecessária à informação sensível e reforça a responsabilização individual. Tal orientação encontra alinhamento com recomendações da (ENISA, 2024), que enfatizam a limitação de privilégios como mecanismo estruturante de mitigação de risco.

Importa salientar que o modelo RBAC constitui a base estrutural do controlo de acessos da plataforma, sendo posteriormente complementado por mecanismos de adaptação contextual, conforme será descrito no subcapítulo 5.4.

### 5.2.2 Camada de Lógica de Negócio - Backend

A camada intermédia do sistema materializa as regras que enquadram o tratamento de dados, assegurando que a execução técnica respeita pressupostos jurídicos previamente definidos. Nesta componente são implementados mecanismos que:

- Confirmam a existência de fundamento legítimo para cada operação de tratamento;
- Vinculam os dados a finalidades determinadas e explicitamente registadas;
- Monitorizam prazos de conservação, acionando alertas ou restrições quando necessário;
- Impedem operações que contrariem princípios como minimização ou limitação da finalidade.

A incorporação destas validações no próprio fluxo aplicacional traduz uma evolução no domínio da engenharia da privacidade, na medida em que desloca o controlo jurídico do plano meramente documental para o plano técnico operacional.

### 5.2.3 Camada de Gestão de Dados

A componente de gestão de dados foi concebida com o objetivo de proteger estruturalmente a informação armazenada. Para tal, foram integrados mecanismos técnicos destinados a reduzir riscos associados a acesso indevido, perda ou utilização incompatível com a finalidade declarada.

Entre as medidas adotadas incluem-se:

- Aplicação de técnicas de cifragem adequadas ao nível de sensibilidade dos dados;

- Recurso à pseudonimização em cenários em que a identificação direta não é estritamente necessária;
- Procedimentos de eliminação segura, prevenindo recuperação posterior indevida;
- Organização lógica da base de dados segundo critérios de finalidade, evitando reutilizações indevidas.

A integração destas salvaguardas desde a fase de desenho encontra-se em consonância com as orientações relativas à proteção de dados desde a concepção e por defeito, reforçando uma abordagem preventiva e não meramente reativa (Comitê Europeu para a Proteção de Dados, 2024).

### 5.2.4 Camada de Auditoria e Conformidade

A camada de auditoria assegura mecanismos de rastreabilidade ao longo de todo o ciclo de vida da informação. A sua função principal consiste em permitir a reconstrução de eventos relevantes para efeitos de controlo interno, responsabilização e eventual supervisão externa.

Neste âmbito, são mantidos:

- Registos estruturados de acessos e alterações;
- Histórico de operações de tratamento;
- Evidência documental de partilhas e eliminações;
- Relatórios consolidados destinados a processos de auditoria.

A capacidade de demonstrar conformidade através de evidência verificável constitui elemento central dos modelos contemporâneos de governação digital, o que identifica o demonstrável como pilar estruturante da gestão responsável de dados.

A Figura 8 representa o modelo conceptual integrado que sustenta a arquitetura da solução proposta, estruturado em três dimensões interdependentes: normativa, tecnológica e organizacional.




***Figura 8 - Modelo Integrado de Governação da Privacidade***

## 5.3 Princípios de Privacidade Integrados

A incorporação dos princípios de proteção de dados no protótipo proposto, assume carácter estruturante e não meramente declarativo. A solução tecnológica foi concebida de modo a internalizar os pressupostos associados à proteção preventiva da informação, refletindo uma abordagem alinhada com as orientações mais recentes das autoridades europeias de supervisão em matéria de proteção de dados, que têm reforçado a necessidade de operacionalização técnica efetiva do princípio da responsabilidade demonstrável (Comitê Europeu para a Proteção de Dados, 2024).

### 5.3.1 Privacy by Design

A proteção desde a concepção materializa-se na integração antecipada de mecanismos de controlo no próprio desenho da arquitetura do sistema. Em vez de tratar a conformidade como um elemento posterior ou corretivo, o modelo proposto incorpora restrições operacionais logo nas fases iniciais de desenvolvimento, em consonância com a crescente ênfase na integração da governação da privacidade na engenharia de sistemas digitais (Hoepman, 2014).

Essa integração traduz-se, desde logo, na realização de uma análise sistemática de riscos antes da implementação funcional do sistema, permitindo identificar potenciais vulnerabilidades associadas ao tratamento previsto. Relatórios recentes sublinham que abordagens baseadas em avaliação prévia de risco constituem elemento central para mitigar incidentes de segurança e reforçar a resiliência digital (ENISA, 2024).

Paralelamente, a definição das categorias de dados a recolher foi orientada por critérios de estrita necessidade, evitando acumulação informacional desproporcional face às finalidades declaradas. A minimização de dados tem sido reiteradamente identificada como mecanismo fundamental de redução estrutural do risco em ambientes digitais complexos (Comitê Europeu para a Proteção de Dados, 2024).

A organização interna da base de dados foi estruturada segundo uma lógica de separação por finalidade, reduzindo a probabilidade de reutilização indevida da informação. Complementarmente, o modelo de autorização adota uma política de privilégios mínimos, limitando o acesso à informação apenas aos perfis cuja intervenção seja funcionalmente justificada, abordagem consistentemente recomendada em relatórios recentes sobre CiberSegurança aplicada (ENISA, 2024).

A geração automática de registos de atividade constitui outro elemento essencial desta abordagem, permitindo demonstrar conformidade de forma objetiva e verificável. A literatura mais recente tem sublinhado que a eficácia do Privacy by Design depende da sua incorporação estrutural na arquitetura do sistema e na documentação técnica de suporte, garantindo auditabilidade e transparência operacional (Comitê Europeu para a Proteção de Dados, 2024).

### 5.3.2 Privacy by Default

De forma complementar, o princípio da proteção de dados por defeito orienta o comportamento inicial da aplicação, assegurando que o estado padrão do sistema corresponde à alternativa menos intrusiva em termos de tratamento de dados pessoais, conforme enfatizado nas orientações europeias recentes sobre configurações seguras por defeito (Comitê Europeu para a Proteção de Dados, 2024).

As configurações iniciais privilegiam a restrição na partilha de informação, evitando que dados sejam automaticamente disponibilizados a terceiros sem intervenção expressa do utilizador. Do mesmo modo, o número de campos obrigatórios foi limitado ao estritamente indispensável ao funcionamento do serviço, prevenindo práticas de recolha excessiva e assegurando a conformidade com recomendações recentes sobre governação de dados e direitos digitais (European Union Agency for Fundamental Rights, 2023).

Os mecanismos de limitação temporal da conservação de dados são ativados automaticamente, impedindo retenção indefinida de informação. Adicionalmente, funcionalidades opcionais que impliquem tratamento adicional de dados permanecem inativas

até que exista manifestação expressa de vontade por parte do utilizador, reforçando a lógica de proteção preventiva.

Relatórios técnicos recentes evidenciam que configurações permissivas por defeito continuam a representar uma das principais fontes de exposição ao risco em aplicações digitais, particularmente em ecossistemas móveis e plataformas orientadas a dados (ENISA, 2024). Assim, a adoção de um modelo restritivo como configuração padrão contribui significativamente para a mitigação preventiva de vulnerabilidades e para o reforço da confiança digital.

### 5.4 Integração do Modelo Oraculum na Gestão de Privacidade

No âmbito da arquitetura desenvolvida, e em complemento ao modelo RBAC anteriormente descrito, foi adotada uma abordagem inspirada no modelo Oraculum, com vista a reforçar uma gestão da privacidade orientada ao contexto e sensível ao comportamento dos utilizadores.

O modelo Oraculum fundamenta-se na capacidade de ajustar, de forma dinâmica, os níveis de acesso à informação, considerando simultaneamente o perfil do utilizador, o contexto de utilização e os padrões de interação ao longo do tempo. Esta abordagem encontra suporte conceptual em trabalhos como os de (Leithardt et al., 2020), que defendem a adaptação contextual das permissões de acesso como mecanismo para modular a exposição da informação em função do ambiente e do comportamento do utilizador.

Em contraste com modelos tradicionais de controlo de acessos, como o Role-Based Access Control (RBAC), que assentam em permissões estáticas previamente definidas, o modelo Oraculum introduz uma lógica adaptativa, na qual as decisões de acesso são determinadas por um conjunto de variáveis contextuais, nomeadamente:

- O perfil do utilizador (por exemplo, turista, operador turístico ou administrador);
- O contexto de acesso, incluindo localização, dispositivo e momento de utilização;
- O histórico de interações e a frequência de utilização da plataforma;
- O nível de sensibilidade associado aos dados envolvidos.

No protótipo proposto, esta abordagem é implementada ao nível da camada de lógica de negócio (backend), através de mecanismos de decisão dinâmica que regulam o acesso à informação. Estes mecanismos refletem a lógica de middleware contextual descrita por (Leithardt et al., 2020), permitindo uma adaptação contínua das permissões em função do contexto e do comportamento observado.

A incorporação deste modelo contribui para a concretização do princípio da minimização de dados, ao restringir o acesso à informação ao estritamente necessário em cada situação. Simultaneamente, reforça a operacionalização do princípio de Privacy by Design, ao integrar mecanismos adaptativos de proteção diretamente na lógica funcional do sistema.

Deste modo, o protótipo desenvolvido evolui para um modelo híbrido de controlo de acessos, que articula a estrutura baseada em papéis do RBAC com a flexibilidade contextual do modelo Oraculum. Esta combinação permite uma gestão mais eficaz, segura e inteligente da privacidade dos dados pessoais, em linha com os desafios atuais dos sistemas digitais orientados à informação.

## 5.5 Modelação do Sistema

A modelação do sistema constitui como um processo técnico e lógico de formalização do protótipo, permitindo a tradução de requisitos normativos e funcionais numa estrutura lógica coerente e verificável. Neste contexto, a modelação não se limita a uma representação meramente descritiva; assume antes uma função estruturante na definição da arquitetura conceptual do sistema e na explicitação das relações ontológicas entre os seus componentes.

Ao operacionalizar o ciclo de vida do tratamento de dados pessoais, a modelação introduz uma perspetiva sistémica orientada por processos, contemplando as diversas operações que incidem sobre os dados, desde a sua recolha e registo até à sua conservação, transmissão, limitação ou eliminação. Esta abordagem permite assegurar o alinhamento entre a dimensão técnica do sistema e o enquadramento jurídico aplicável, incorporando princípios estruturantes como a responsabilidade, a limitação das finalidades, a minimização de dados e a integridade e confidencialidade da informação.

Sob o ponto de vista metodológico, a modelação promove a redução de ambiguidades semânticas, clarifica fronteiras de responsabilidade e favorece a rastreabilidade das operações de tratamento. Assim, constitui um instrumento de governação organizacional e de mitigação de risco, ao permitir antecipar vulnerabilidades estruturais e pontos de fricção normativa antes da implementação efetiva do protótipo.

### 5.5.1 Diagramas Conceptuais

Os diagramas conceptuais assumem, neste enquadramento, a função de abstração formal das entidades nucleares do ecossistema de tratamento de dados e das relações estruturais que entre elas se estabelecem. Trata-se de uma representação ontológica que visa capturar não

apenas objetos ou atores isolados, mas, sobretudo, as interdependências funcionais e jurídicas que configuram o sistema como um todo coerente.

No plano conceptual, identificam-se como entidades estruturantes:

- Titular dos Dados, enquanto sujeito de direitos fundamentais associados à proteção da sua esfera informacional;
- Responsável pelo Tratamento, enquanto entidade que determina as finalidades e os meios do tratamento;
- Sistema de Gestão, entendido como infraestrutura tecnológica e organizacional que operacionaliza o tratamento;
- Dados Pessoais, enquanto unidade informacional suscetível de identificação direta ou indireta;
- Finalidade do Tratamento, que delimita o âmbito material da utilização dos dados;
- Base Legal, enquanto fundamento legitimador da licitude do tratamento;
- Destinatários Terceiros, que intervêm no ecossistema informacional mediante comunicação ou acesso autorizado.

A representação diagramática destas entidades permite evidenciar relações de dependência, hierarquias decisórias e fluxos de circulação da informação, promovendo uma leitura integrada entre dimensão técnica e dimensão normativa. Mais do que um instrumento gráfico, o diagrama conceptual constitui um modelo lógico formal que sustenta a coerência interna do sistema e assegura consistência entre arquitetura tecnológica e exigências jurídicas.

Adicionalmente, a formalização destas relações favorece a identificação de pontos críticos de controlo designadamente momentos de recolha, transmissão ou partilha de dados que exigem salvaguardas acrescidas em termos de segurança, transparência e responsabilização. Deste modo, os diagramas conceptuais desempenham um papel fundamental na consolidação de uma abordagem preventiva à proteção de dados, integrando o princípio da proteção de dados desde a concepção (privacy by design) na própria estrutura do protótipo.

A modelação conceptual não apenas organiza os elementos constitutivos do sistema, mas estabelece um quadro analítico que sustenta a sua legitimidade jurídica, robustez estrutural e sustentabilidade operacional.

### 5.6 Ciclo de Vida do Tratamento de Dados Pessoais

O tratamento de dados pessoais deve ser analisado enquanto processo estruturado, composto por um conjunto de fases sequenciais que asseguram coerência funcional, conformidade

jurídica e controlo organizacional. A adoção de uma perspetiva de ciclo de vida permite integrar requisitos legais, procedimentos internos e mecanismos tecnológicos numa lógica de governação orientada à mitigação de risco e à responsabilização institucional.

A primeira fase corresponde à recolha dos dados. Esta deve ocorrer com base numa finalidade previamente determinada, explícita e legítima. O titular deve ser informado de forma clara quanto à identidade do responsável pelo tratamento, às finalidades subjacentes, aos direitos que lhe assistem e às condições de exercício desses direitos. Do ponto de vista da gestão da informação, a recolha deve respeitar critérios de adequação e proporcionalidade, limitando-se aos elementos estritamente necessários à prossecução do objetivo definido.

Subsequentemente, procede-se à validação do fundamento jurídico que legitima o tratamento. A existência de uma base legal adequada constitui condição necessária para a continuidade do processo. Esta pode assentar, entre outros pressupostos, no consentimento do titular dos dados, na execução de um contrato, no cumprimento de obrigação jurídica ou na prossecução de interesses legítimos, desde que devidamente ponderados. Esta etapa assume uma natureza preventiva, funcionando como mecanismo de controlo.

Após a validação jurídica, os dados são registados nos sistemas de informação da organização, sendo classificados de acordo com a finalidade associada. A categorização estruturada contribui para assegurar a segregação lógica da informação e facilitar mecanismos de auditoria e monitorização. Simultaneamente, permite alinhar os níveis de acesso e os perfis de utilizador com as necessidades operacionais identificadas.

A fase de armazenamento implica a implementação de medidas técnicas e organizativas adequadas ao risco. Estas incluem, designadamente, mecanismos de autenticação e controlo de acessos, cifragem da informação, registo de eventos, definição de políticas internas de segurança e formação dos colaboradores. A adoção destas medidas visa salvaguardar a integridade, disponibilidade e confidencialidade dos dados ao longo do respetivo período de conservação.

A utilização dos dados deve permanecer circunscrita à finalidade que justificou a sua recolha. Qualquer utilização subsequente incompatível com o propósito inicial exige reavaliação do enquadramento jurídico e, quando aplicável, a obtenção de novo fundamento legitimador. Este controlo contínuo reforça a previsibilidade do tratamento e reduz o risco de desvios funcionais.

Sempre que ocorra comunicação de dados a terceiros, a mesma deve ser enquadrada por instrumentos jurídicos adequados, que definam responsabilidades, limites de utilização e requisitos de segurança. A partilha deve obedecer a critérios de necessidade e

proporcionalidade, garantindo que apenas são transmitidos os dados estritamente indispensáveis à finalidade em causa.

Por último, o ciclo de vida do tratamento inclui a fase de conservação e subsequente eliminação ou anonimização. A retenção deve limitar-se ao período necessário para cumprimento da finalidade ou de obrigações legais aplicáveis. Decorrido esse prazo, os dados devem ser eliminados de forma segura ou transformados de modo irreversível, impedindo a identificação dos titulares.

A articulação destas fases evidencia a interdependência entre arquitetura tecnológica, processos organizacionais e enquadramento normativo. No contexto da Informática de Gestão, esta abordagem reforça a importância de modelos de governação de dados que assegurem de forma simultânea conformidade regulatória, eficiência operacional e controlo do risco.

## 5.7 Implementação do Protótipo

A implementação do artefacto resultou no desenvolvimento de um protótipo funcional da plataforma GoCaboVerde, concebida para demonstrar a aplicação prática dos requisitos funcionais e não funcionais identificados nas fases anteriores da investigação. O protótipo integra funcionalidades orientadas para a exploração de destinos e serviços turísticos, articuladas com mecanismos de autenticação, gestão de dados pessoais, controlo da privacidade, gestão do consentimento e exercício dos direitos dos titulares dos dados.[1]

A conceção das interfaces procurou privilegiar uma experiência de utilização simples e intuitiva, permitindo que as funcionalidades associadas à proteção de dados sejam disponibilizadas de forma integrada no percurso de interação do utilizador com a plataforma. Esta abordagem demonstra a incorporação de requisitos de privacidade na conceção de uma solução digital orientada para o turismo, em conformidade com os princípios de Privacy by Design e Privacy by Default.

[1] O conjunto completo de interfaces e demais elementos do protótipo GoCaboVerde encontra-se disponível no repositório público do projeto no GitHub: https://github.com/heniopina/Um-Estudo-de-Caso-em-Cabo-Verde-com-Utiliza-o-de-Privacidade-de-Dados

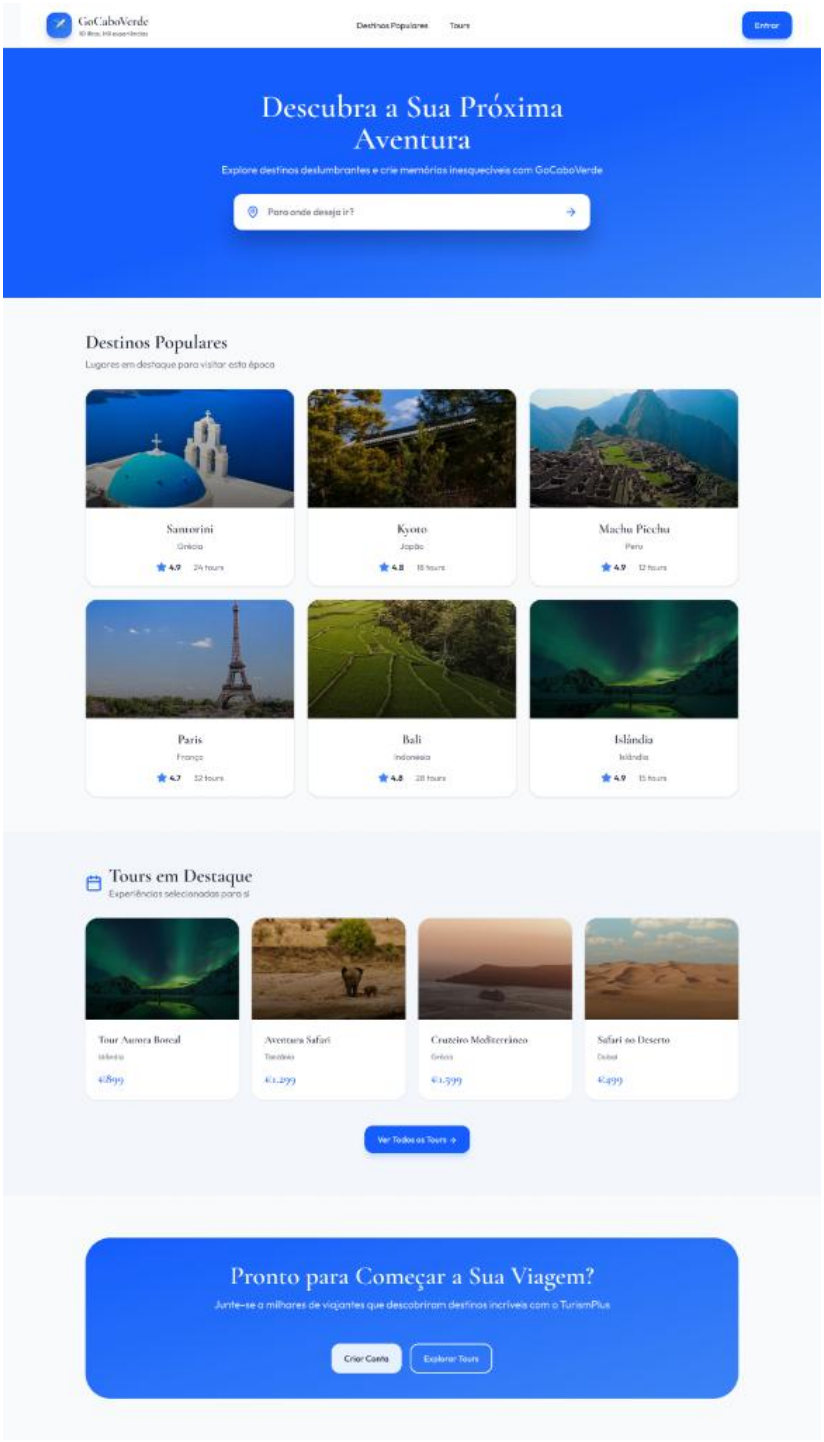



***Figura 9 - Página inicial do protótipo GoCaboVerde***

A Figura 9 apresenta a página inicial da plataforma GoCaboVerde, principal ponto de entrada para a exploração dos serviços disponibilizados. A interface permite pesquisar destinos turísticos, consultar destinos populares e aceder aos tours em destaque, procurando proporcionar uma navegação simples e intuitiva.

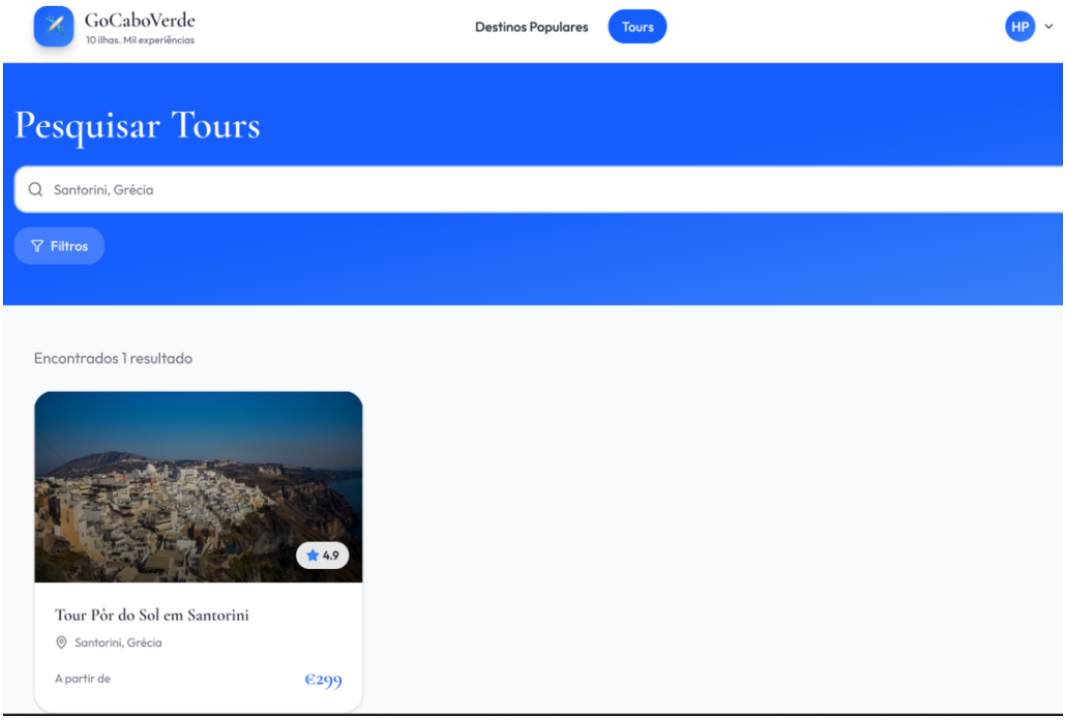



*Figura 10 - Interface de pesquisa e consulta de tours*

A Figura 10 apresenta a funcionalidade de pesquisa de tours, através da qual o utilizador pode introduzir um destino e consultar os resultados disponíveis. A interface integra mecanismos de pesquisa e filtragem e apresenta informação relevante sobre as ofertas turísticas, incluindo localização, avaliação e preço.

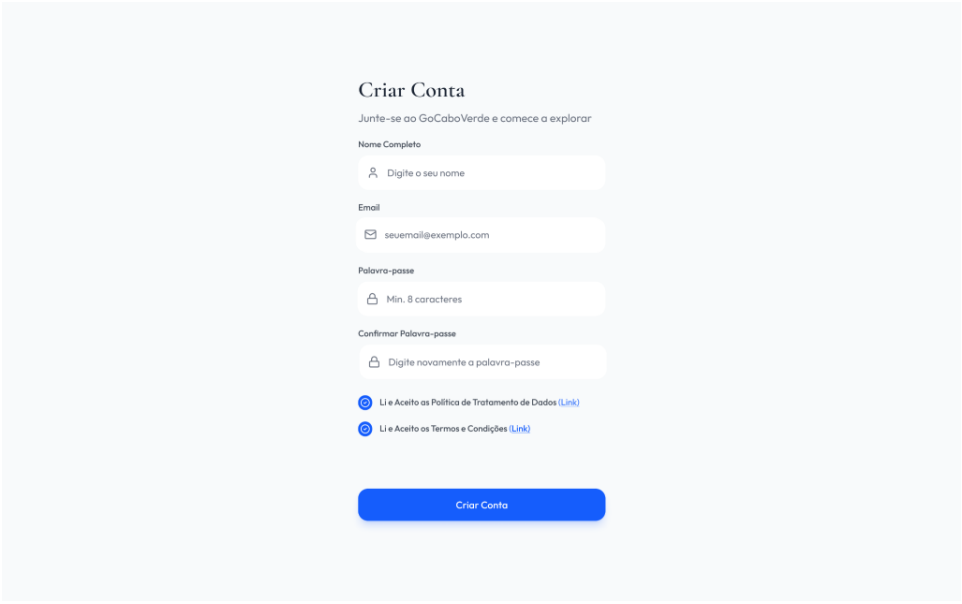



*Figura 11 - Interface de criação de conta e aceitação das condições de tratamento de dados*

A Figura 11 apresenta o processo de criação de uma conta. São solicitados os dados necessários ao registo, nomeadamente nome, endereço de correio eletrónico e palavra-passe. A interface disponibiliza ainda o acesso à Política de Tratamento de Dados e aos Termos e Condições, contribuindo para a transparência e informação do titular.




***Figura 12 - Interface de autenticação do utilizador***

A Figura 12 apresenta a interface de autenticação, através da qual os utilizadores registados podem aceder à respetiva área pessoal mediante endereço de correio eletrónico e palavra-passe. Este mecanismo contribui para o controlo de acesso às funcionalidades e informações reservadas.

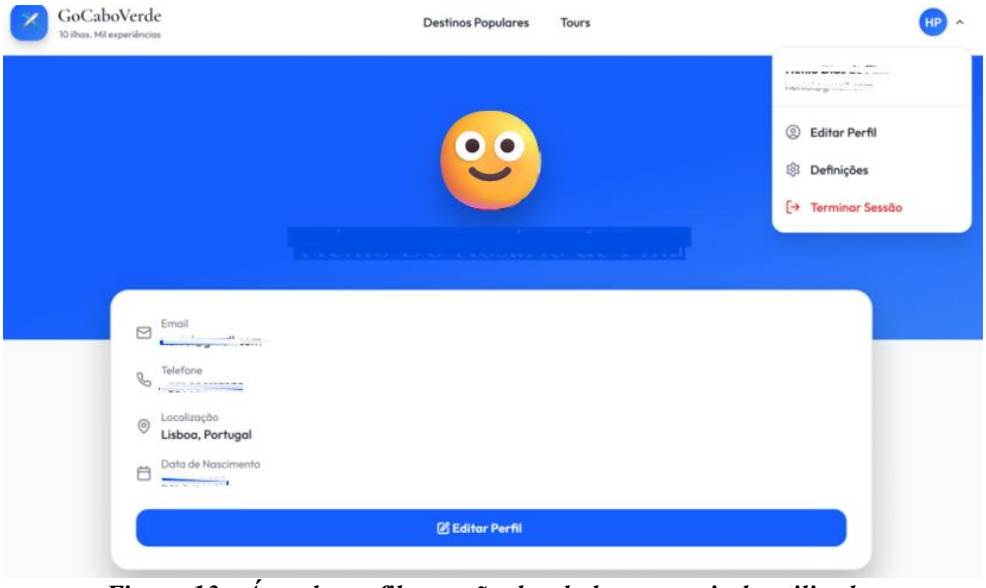



*Figura 13 - Área de perfil e gestão dos dados pessoais do utilizador*

A Figura 13 apresenta a área de perfil, na qual são disponibilizados os dados associados à conta e funcionalidades destinadas à respetiva gestão. A possibilidade de edição permite ao titular manter os dados atualizados e aceder às configurações relacionadas com a conta e a privacidade.

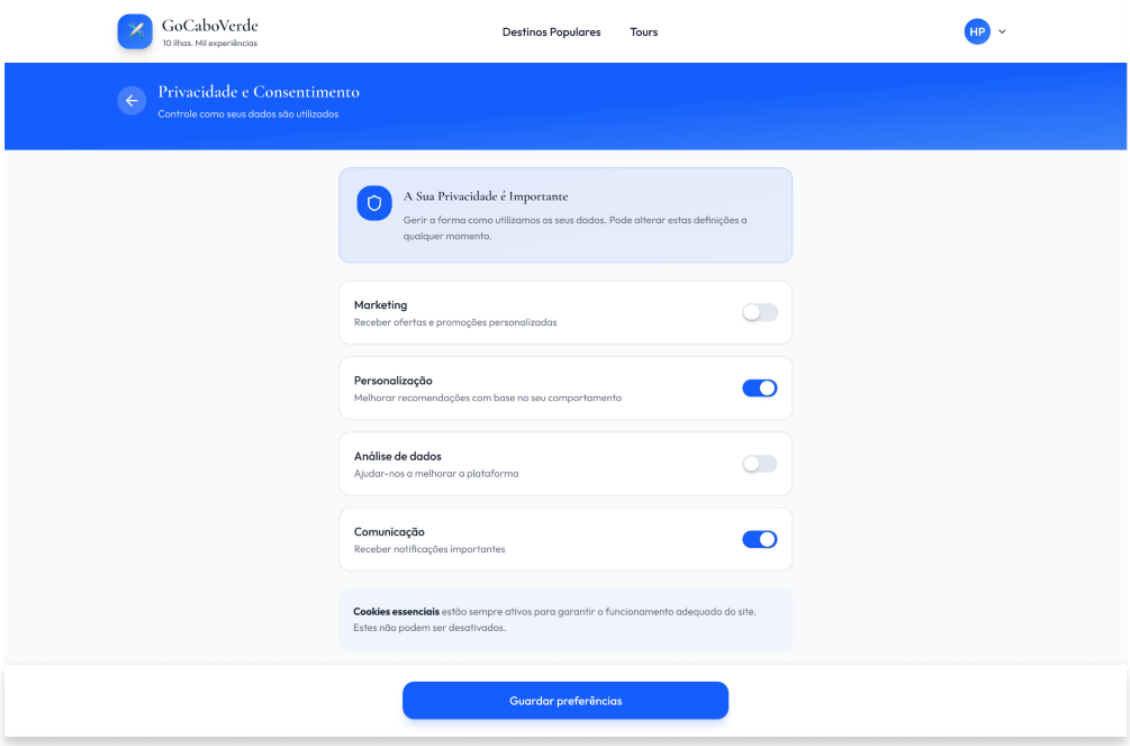



*Figura 14 - Interface de gestão da privacidade e do consentimento*

A Figura 14 apresenta a área dedicada à gestão da privacidade e do consentimento. O utilizador pode controlar finalidades distintas, como marketing, personalização, análise de dados e comunicação, gerindo individualmente as suas preferências. Esta funcionalidade materializa princípios de transparência, controlo do titular e proteção de dados por defeito.

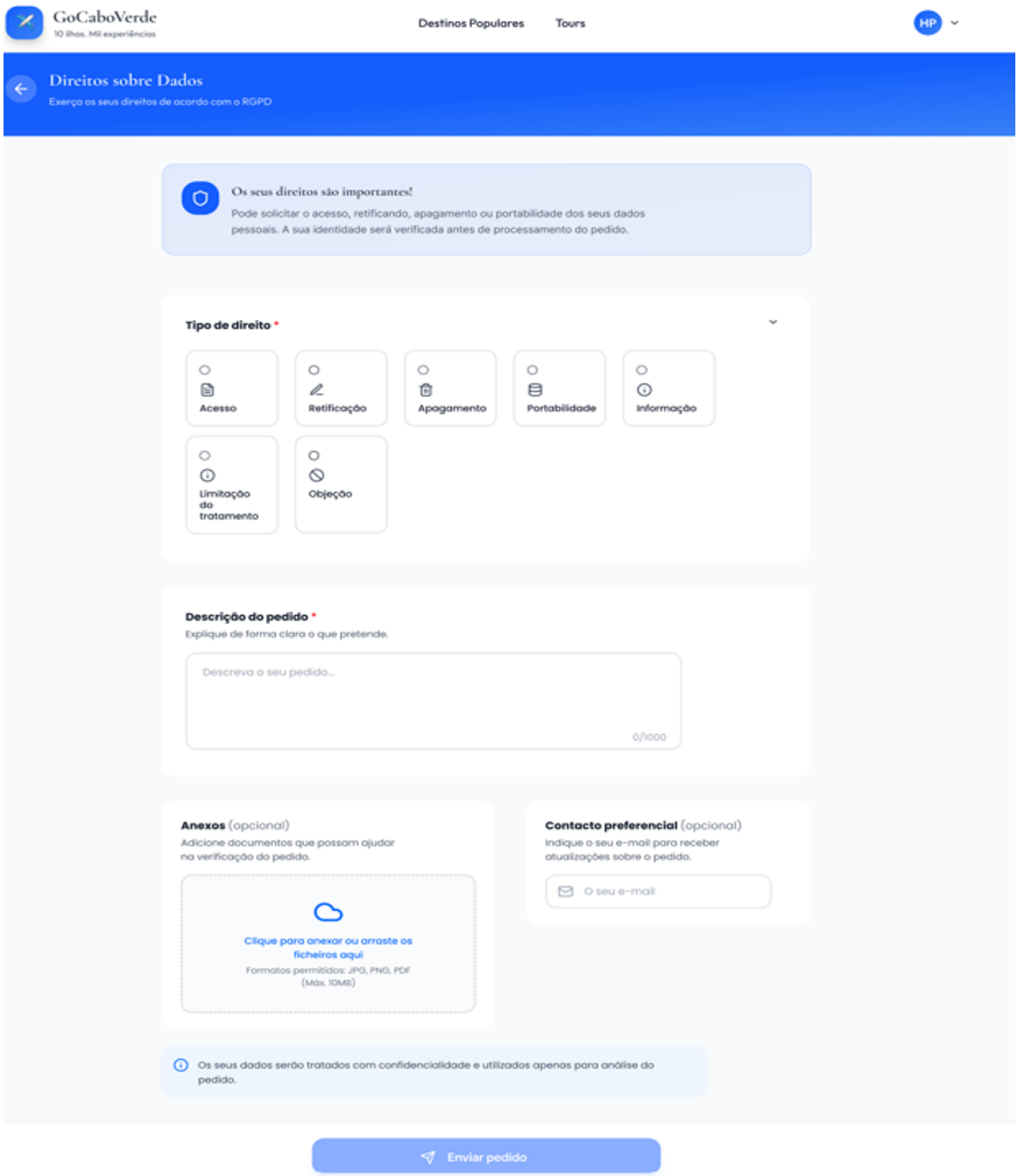



***Figura 15 - Interface para o exercício dos direitos do titular dos dados***

A Figura 15 apresenta a funcionalidade destinada ao exercício dos direitos dos titulares dos dados pessoais. O utilizador pode selecionar direitos como acesso, retificação, apagamento,

portabilidade, informação, limitação do tratamento e oposição, descrever o pedido e, quando necessário, anexar documentação complementar.

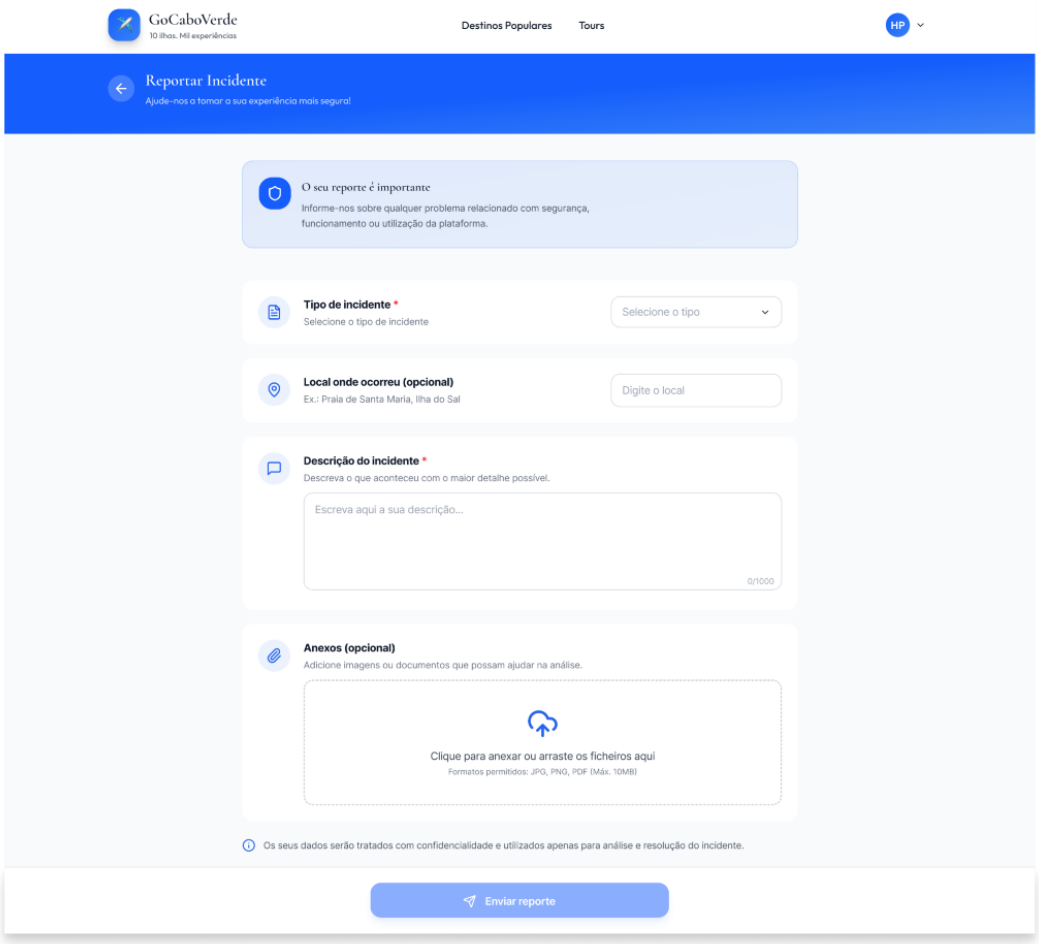



***Figura 16 - Interface para comunicação de incidentes***

A Figura 16 apresenta a funcionalidade destinada à comunicação de incidentes relacionados com a utilização da plataforma. O utilizador pode selecionar o tipo de incidente, indicar opcionalmente o local, descrever a ocorrência e anexar elementos relevantes. A informação sobre a finalidade do tratamento reforça a transparência do processo.

A apresentação das interfaces desenvolvidas demonstra a concretização funcional do artefacto e a integração entre as componentes associadas à atividade turística e os mecanismos de proteção de dados pessoais. O protótipo incorpora funcionalidades de pesquisa e consulta de serviços turísticos, autenticação, gestão do perfil, controlo das preferências de privacidade, gestão do consentimento, exercício dos direitos dos titulares e comunicação de incidentes.

Neste sentido, o artefacto constitui uma demonstração prática da possibilidade de integrar requisitos de privacidade e proteção de dados no processo de conceção de plataformas digitais

destinadas ao setor do turismo. As funcionalidades implementadas procuram evidenciar a operacionalização dos princípios de Privacy by Design e Privacy by Default, estabelecendo uma ligação entre os requisitos identificados, a arquitetura proposta e a sua materialização no protótipo.

## 5.8 Especificação Técnica do Protótipo

A utilização do protótipo requer um ambiente com requisitos mínimos definidos tanto no software como do hardware, para que possa suportar a execução. Recomenda-se um sistema com, no mínimo, 8 GB de memória RAM, processador equivalente a Intel i5 e capacidade de armazenamento adequada à utilização da aplicação. O dispositivo deve dispor de um navegador web moderno compatível com Google Chrome, Mozilla Firefox ou Microsoft Edge com padrões HTML5, CSS3 e JavaScript. O utilizador deve ainda ter uma ligação à Internet estável, essencial para a comunicação contínua com o servidor da aplicação e para a execução de processos como registo, autenticação, consulta de serviços e gestão de dados pessoais. Não é necessária a instalação do protótipo, uma vez que este se encontra acessível através de um navegador, sendo apenas exigido o consentimento informado para o tratamento de dados pessoais, em conformidade com os requisitos de privacidade implementados no sistema.

# CAPÍTULO 6

## Avaliação do Protótipo

### 6.1 Enquadramento da Avaliação do Protótipo

O capítulo apresenta os resultados da avaliação do protótipo desenvolvido no âmbito desta investigação, cujo principal objetivo consiste em analisar a perceção dos utilizadores relativamente à usabilidade, transparência, privacidade, proteção de dados e confiança associadas ao protótipo proposto.

A avaliação do protótipo desenvolvido representa uma das etapas fundamental da metodologia Design Science Research (DSR), permitindo validar a relevância e adequação da solução proposta face ao problema identificado na investigação. Neste contexto, pretende-se verificar se a integração de mecanismos orientados para a proteção de dados pessoais contribui positivamente para a experiência dos utilizadores e para o aumento da confiança em serviços digitais turísticos.

A avaliação foi realizada com base na interação dos participantes com o protótipo desenvolvido no ambiente simulado, seguida da aplicação de um questionário através de Google Forms com questões fechadas e abertas. O instrumento de recolha de dados permitiu analisar dimensões relacionadas com:

- Usabilidade;
- Transparência das informações;
- Privacidade;
- Confiança;
- Controlo dos dados pessoais;
- Intenção de utilização.

Os resultados obtidos permitem compreender de que forma os utilizadores percecionam os mecanismos de proteção de dados integrados em aplicações turísticas digitais, contribuindo para responder à questão de investigação proposta.

Segundo (Peffers et al., 2007), a fase de avaliação na metodologia DSR assume particular relevância, na medida em que permite aferir o desempenho, utilidade e adequação do artefacto desenvolvido ao contexto de aplicação.

## 6.2 Metodologia de Avaliação

### 6.2.1 Abordagem Metodológica

A avaliação do protótipo adotou uma abordagem predominantemente quantitativa, complementada por elementos qualitativos obtidos através de questões abertas incluídas no questionário aplicado aos participantes.

A abordagem quantitativa permitiu analisar as perceções dos utilizadores relativamente às funcionalidades da aplicação e aos mecanismos de privacidade e proteção de dados implementados. Por sua vez, as questões abertas possibilitaram recolher opiniões, sugestões e comentários adicionais acerca da experiência de utilização.

A metodologia adotada encontra-se alinhada com os princípios da Design Science Research (DSR), particularmente nas fases de demonstração e avaliação do artefacto.

De acordo com (Hevner et al., 2004), a DSR procura desenvolver soluções tecnológicas inovadoras capazes de responder a problemas concretos, sendo a avaliação um elemento essencial para validar a utilidade do artefacto produzido.

### 6.2.2 Instrumentos de Recolha de Dados

Para a recolha de dados foi desenvolvido um questionário estruturado composto por cinco secções principais:

1. Caracterização do participante;
2. Perceção sobre privacidade e proteção de dados;
3. Avaliação do protótipo;
4. Avaliação global da solução;
5. Questões abertas.

As questões fechadas foram estruturadas com recurso à escala de Likert de cinco pontos, variando entre:

1 - Discordo totalmente

2 - Discordo

3 - Nem concordo nem discordo

4 - Concordo

5 - Concordo totalmente

A utilização da escala de Likert permitiu medir o grau de concordância dos participantes relativamente às dimensões avaliadas.

A escala de Likert é amplamente utilizada em estudos de perceção e comportamento, permitindo analisar atitudes, opiniões e níveis de concordância de forma estruturada (SGOBBI et al., 2024).

### 6.2.3 Participantes

Os participantes do estudo corresponderam a utilizadores com experiência ou familiaridade com plataformas digitais relacionadas com o setor do turismo. A participação foi voluntária, anónima e confidencial, sendo os dados recolhidos utilizados exclusivamente para fins académicos, em conformidade com os princípios éticos aplicáveis à investigação científica.

### 6.2.4 Procedimento de avaliação

O processo de avaliação decorreu em diferentes etapas.

Inicialmente, foi apresentada aos participantes uma demonstração do protótipo desenvolvido, destacando-se as principais funcionalidades relacionadas com:

- Navegação;
- Gestão de consentimento;
- Transparência relativamente à recolha de dados;
- Opções de privacidade;
- Mecanismos de controlo de dados pessoais.

Após a demonstração e utilização da aplicação, os participantes procederam ao preenchimento do questionário de avaliação.

Os dados recolhidos foram posteriormente organizados e analisados com recurso a técnicas estatísticas descritivas.

### 6.2.5 Técnicas de análise de dados

A análise dos dados recolhidos foi realizada através de:

- Estatística descritiva;
- Análise por dimensões;
- Análise de consistência interna;
- Análise qualitativa das respostas abertas.

A consistência interna do instrumento poderá ser verificada através do Alpha de Cronbach, permitindo analisar a fiabilidade das dimensões do questionário.

Segundo (Rego Monteiro da Hora et al., 2010), o Alpha de Cronbach constitui um dos indicadores estatísticos mais utilizados para avaliar a consistência interna de instrumentos de recolha de dados baseados em escalas.

As respostas abertas foram analisadas através de análise temática, permitindo identificar os principais padrões e perceções dos participantes.

## 6.3 Caracterização da Amostra

A presente secção apresenta a caracterização dos participantes envolvidos no processo de avaliação do protótipo.

A análise da amostra incidiu sobre:

- Faixa etária;
- Género;
- Nível de formação académica.

Os resultados obtidos permitem compreender o perfil dos participantes e contextualizar as perceções apresentadas relativamente à solução proposta

### 6.3.1 Faixa etária

**Tabela 20 - Distribuição da amostra por faixa etária**

| Faixa Etária | Frequência | Percentagem |
|---|---|---|
| 18-24 | 2 | 18,2% |
| 25-34 | 2 | 18,2% |
| 35-44 | 4 | 36,4% |
| 45-54 | 1 | 9,1% |
| 55 ou mais | 2 | 18,2% |
| **Total** | **11** | **100%** |

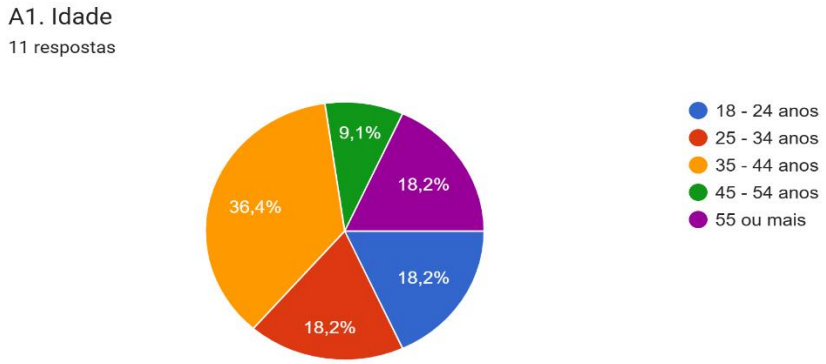



***Figura 17 - Distribuição da amostra por faixa etária.***

Os resultados demonstram uma predominância de utilizadores pertencentes à faixa etária entre os 35 e os 44 anos, representando uma amostra de 36.4%.

Observa-se igualmente a participação de diferentes grupos etários, permitindo obter perceções diversificadas relativamente à utilização de aplicações turísticas e à proteção de dados pessoais.

### 6.3.2 Género

**Tabela 21 - Distribuição da amostra por género**

| Género | Frequência | Percentagem |
|---|---|---|
| Feminino | 8 | 72.7% |
| Masculino | 3 | 27.3% |
| **Total** | **11** | **100%** |

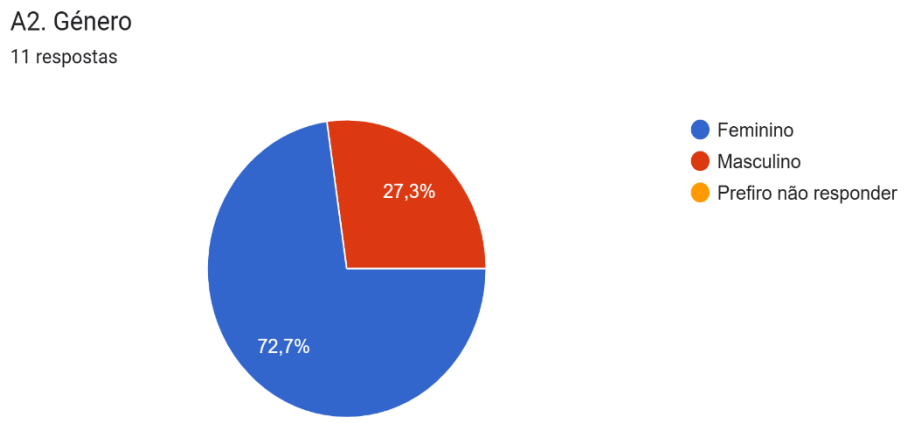



***Figura 18 - Distribuição da amostra por género***

Relativamente ao género, verificou-se predominância de participantes do género feminino com uma amostra de 72.7%.

### 6.3.3 Formação Académica

**Tabela 22 - Distribuição da amostra por habilitações académicas**

| Habilitações Académicas | Frequência | Percentagem |
|---|---|---|
| Licenciatura | 3 | 27.3% |
| Mestrado | 7 | 63.6% |
| Outro | 1 | 9.1% |
| **Total** | **11** | **100%** |

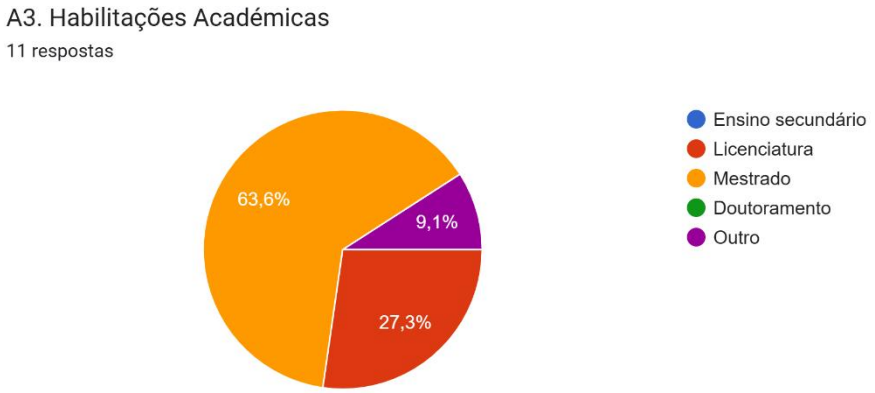



***Figura 19 - Distribuição da amostra por habilitações académicas***

Os resultados evidenciam predominância de participantes com grau de mestrado, representando 63.7% da amostra.

O elevado nível de formação académica poderá contribuir para uma maior sensibilidade relativamente às questões associadas à privacidade e proteção de dados em ambientes.

## 6.4 Análise Descritiva dos Resultados

A presente secção apresenta a análise descritiva das respostas obtidas relativamente às diferentes dimensões avaliadas no questionário.

Para facilitar a interpretação dos resultados, as questões foram agrupadas em dimensões analíticas.

### 6.4.1 Perceção sobre privacidade e proteção de dados

Esta dimensão teve como objetivo avaliar a importância atribuída pelos participantes à privacidade e proteção dos dados pessoais no contexto da utilização de aplicações digitais de turismo.

As questões analisadas nesta dimensão correspondem a:

- B1 – Considero importante que aplicações turísticas protejam os dados pessoais dos utilizadores.
- B2 – Costumo preocupar-me com a forma como os meus dados pessoais são utilizados em plataformas digitais.
- B3 – Sinto maior confiança em aplicações que apresentam informações claras sobre privacidade.
- B4 – O consentimento para recolha de dados deve ser apresentado de forma clara e transparente.
- B5 – Os utilizadores devem ter controlo sobre os seus dados pessoais em aplicações digitais.

**Tabela 23 - Médias da Dimensão Perceção sobre Privacidade e Proteção de Dados**

| Questão | Média |
|---|---|
| B1 | 4.63 |
| B2 | 4.27 |
| B3 | 4.36 |
| B4 | 4.60 |
| B5 | 4.45 |
| **Média Global da Dimensão** | **4.47** |

Os resultados obtidos evidenciam uma perceção globalmente muito positiva relativamente à importância da privacidade e proteção de dados pessoais em aplicações digitais de turismo, registando uma média global de 4,47 numa escala de 1 a 5.

### 6.4.2 Avaliação do protótipo

1. Usabilidade

A dimensão da Usabilidade procurou avaliar a facilidade de utilização, navegação e compreensão das funcionalidades da aplicação.

As questões analisadas nesta dimensão correspondem a:

- AP1 - O protótipo foi fácil de utilizar;
- AP2 - A navegação na aplicação foi clara e intuitiva;

- AP3 - As funcionalidades disponíveis foram fáceis de compreender.

**Tabela 24 - Resultados da dimensão Usabilidade**

| Questão | Média |
|---|---|
| AP1 | 3.8 |
| AP2 | 3.8 |
| AP3 | 3.9 |
| **Média Global da Dimensão** | **3.83** |

A dimensão Usabilidade apresentou uma média global de 3.83, correspondendo a uma avaliação positiva por parte dos participantes.

Os resultados sugerem que os utilizadores consideraram a aplicação relativamente fácil de utilizar, com uma navegação compreensível e funcionalidades acessíveis. Apesar da avaliação positiva, os resultados indicam a possibilidade de introdução de melhorias adicionais ao nível da experiência de utilização e da interface da aplicação.

Segundo (Jakob Nielsen, 1994), a usabilidade constitui um dos fatores mais relevantes para a aceitação e adoção de sistemas digitais pelos utilizadores.

2. Transparência e Privacidade

A dimensão da Transparência e Privacidade avaliou a clareza das informações relacionadas com recolha de dados, mecanismo de consentimento e opções de privacidade.

As questões analisadas nesta dimensão correspondem a:

- AP4 - O sistema apresentou informações claras sobre o tratamento dos dados pessoais;
- AP5 - As opções relacionadas com privacidade estavam facilmente visíveis;
- AP6 - Consegui compreender quais dados pessoais seriam recolhidos;
- AP8 - O protótipo aparenta respeitar princípios de privacidade e proteção de dados;
- AP9 - Senti que possuía controlo sobre os meus dados pessoais durante a utilização.

**Tabela 25 - Resultados da dimensão Transparência e Privacidade**

| Questão | Média |
|---|---|
| AP4 | 4.09 |
| AP5 | 4.09 |
| AP6 | 4.0 |
| AP8 | 4.0 |
| AP9 | 4.27 |
| **Média Global da Dimensão** | **4.09** |

A dimensão Transparência e Privacidade apresentou uma média global de 4.09, correspondendo a uma avaliação positiva por parte dos participantes. O que indica que os participantes reconheceram a existência de mecanismos claros de transparência e proteção de dados no protótipo.

A perceção positiva relativamente ao controlo dos dados pessoais demonstra a importância da integração de funcionalidades orientadas à privacidade em aplicações digitais turísticas.

3. Confiança

A dimensão da Confiança procurou avaliar a confiança transmitido pelo protótipo.

As questões analisadas nesta dimensão correspondem a:

- AP7 - O protótipo transmitiu confiança durante a utilização;
- AP10 - A utilização do protótipo aumentaria a minha confiança em serviços digitais de turismo.

**Tabela 26 - Resultados da dimensão Confiança**

| Questão | Média |
|---|---|
| AP7 | 4.0 |
| AP10 | 4.18 |
| **Média Global da Dimensão** | **4.09** |

A dimensão Confiança apresentou uma média global de 4.09, correspondendo a uma avaliação positiva por parte dos participantes. O que demonstra que os mecanismos de privacidade e proteção de dados implementados contribuíram positivamente para a confiança dos utilizadores. A confiança é um elemento essencial para adoção de serviços digitais no setor do turismo.

4. Intenção de Uso

Esta dimensão avaliou a predisposição dos participantes para utilizar a aplicação num contexto real.

As questões analisadas nesta dimensão correspondem a:

- AP11 - Utilizaria uma aplicação semelhante num contexto real.

**Tabela 27 - Resultados da dimensão Intenção de Uso**

| Questão | Média |
|---|---|
| AP11 | 4.36 |
| **Média Global da Dimensão** | **4.36** |

A dimensão Intenção de Uso apresentou uma média global de 4.36, o que corresponde a uma avaliação positiva, e uma elevada intenção de utilização da solução proposta, evidenciando a aceitação do protótipo pelos participantes.

### 6.4.3 Avaliação global do protótipo

**Tabela 28 - Médias da Dimensão Avaliação Global do Protótipo**

| Questão | Média |
|---|---|
| AG1 | 4.36 |
| AG2 | 4.36 |
| AG3 | 4.27 |
| AG4 | 4.36 |
| AG5 | 4.36 |
| AG6 | 4.45 |
| **Média Global da Dimensão** | **4.36** |

Os resultados obtidos demonstram uma avaliação global positiva da solução proposta.

A média global de 4.36 evidencia que os participantes reconheceram a relevância dos mecanismos implementados para proteção dos dados pessoais, bem como a clareza das informações disponibilizadas e a confiança transmitida durante a utilização da aplicação.

Os resultados sugerem que a incorporação de princípios de privacidade e proteção de dados contribuiu significativamente para a perceção positiva do protótipo desenvolvido.

## 6.5 Consistência Interna do Instrumento

A consistência interna do instrumento poderá ser avaliada através do cálculo do Alpha de Cronbach, permitindo verificar a fiabilidade das dimensões analisadas.

O Alpha de Cronbach representa um dos indicadores mais utilizados para avaliar a consistência interna de questionários baseados em escalas de Likert.

Os valores de referência geralmente aceites são:

- Superior a 0,90 - excelente;
- Entre 0,80 e 0,90 - muito bom;
- Entre 0,70 e 0,79 - aceitável;
- Inferior a 0,60 - consistência reduzida.

**Tabela 29 - Resultados do Coeficiente Alpha de Cronbach**

| Dimensão | Nº de Itens | Alpha |
|---|---|---|
| Usabilidade | 3 | 0.640 |
| Transparência e Privacidade | 5 | 0.856 |
| Confiança | 2 | 0.830 |

Os resultados demonstram níveis adequados de consistência interna para as dimensões analisadas.

A dimensão Usabilidade apresentou um valor de $\alpha = 0,64$. Embora inferior aos restantes resultados, este valor é considerado aceitável em estudos exploratórios com amostras reduzidas, como é o caso da presente investigação. A dimensão Confiança apresentou igualmente um valor elevado ($\alpha = 0,830$), indicando uma forte coerência entre as questões analisadas.

Por sua vez, a dimensão Transparência e Privacidade apresentou o valor mais elevado ($\alpha = 0,856$), evidenciando uma consistência interna muito boa entre os itens utilizados.

De forma geral, os resultados obtidos permitem concluir que o instrumento apresenta níveis satisfatórios de fiabilidade para a avaliação do protótipo desenvolvido.

## 6.6 Análise Qualitativa da Respostas Abertas

A análise das respostas abertas permitiu identificar os principais aspectos valorizados pelos participantes e as sugestões de melhoria apresentadas.

### 6.6.1 Aspectos positivos

- Transparência;
- Controlo dos dados pessoais;
- Facilidade de utilização;
- Confiança;
- Clareza das informações

### 6.6.2 Sugestões de melhorias

- Inclusão de novas funcionalidades;
- Realidade aumentada;
- Melhorias na interface;
- Mecanismos adicionais de apoio ao utilizador.

Os resultados qualitativos reforçam as conclusões obtidas na análise quantitativa.

# Capítulo 7

# Conclusões e recomendações

## 7.1 Principais conclusões

A presente investigação teve como principal objetivo desenvolver e avaliar uma aplicação turística digital incorporando princípios de privacidade e proteção de dados, considerando o contexto do turismo digital em Cabo Verde e os referenciais normativos aplicáveis.

A investigação permitiu identificar a crescente importância da proteção de dados pessoais no contexto da digitalização do setor do turismo. O aumento da utilização de plataformas digitais turísticas implica desafios significativos relacionados com:

- Recolha de dados pessoais;
- Transparência;
- Consentimento;
- Segurança da informação;
- Confiança digital.

Com base nos princípios da Design Science Research (DSR), foi desenvolvido um protótipo de aplicação turística digital orientado para a integração de mecanismos de privacidade e proteção de dados.

A avaliação realizada demonstrou que os participantes reconheceram positivamente:

- A usabilidade da aplicação;
- A clareza das informações;
- Os mecanismos de consentimento;
- A transparência relativamente ao tratamento de dados;
- O controlo disponibilizado aos utilizadores;
- A confiança transmitida pela solução.

Os resultados obtidos sugerem que a incorporação de mecanismos de privacidade e proteção de dados pode aumentar a confiança dos utilizadores em serviços digitais turísticos.

A investigação permitiu igualmente demonstrar que os princípios de proteção de dados podem ser integrados desde as fases iniciais de desenvolvimento de aplicações digitais, contribuindo para soluções mais transparentes, éticas e orientadas para o utilizador.

## 7.2 Limitações do Estudo

Apesar dos contributos alcançados, a investigação apresenta algumas limitações que devem ser consideradas. Uma das principais limitações relaciona-se com a dimensão da amostra utilizada na avaliação do protótipo. O número reduzido de participantes poderá limitar a generalização dos resultados obtidos.

Outra limitação prende-se com o facto de a avaliação ter sido realizada em ambiente controlado, não correspondendo a uma implementação real da aplicação em contexto operacional.

Adicionalmente, a investigação concentrou-se no contexto do turismo digital em Cabo Verde, podendo existir diferenças culturais, tecnológicas e regulatórias noutros contextos geográficos.

A limitação temporal da investigação também condicionou a possibilidade de realizar avaliações prolongadas sobre o comportamento dos utilizadores ao longo do tempo.

## 7.3 Recomendações para Investigação Futura

Com base nos resultados obtidos e nas limitações identificadas, recomenda-se que futuras investigações possam:

- Realizar testes em ambientes reais de utilização;
- Aumentar a dimensão da amostra;
- Incluir diferentes perfis de turistas;
- Analisar impactos culturais na perceção de privacidade;
- Integrar mecanismos avançados de segurança e autenticação;
- Explorar a utilização de inteligência artificial para personalização de serviços turísticos;
- Analisar modelos de proteção de dados baseados em blockchain;
- Comparar diferentes abordagens de consentimento e transparência.

Sugere-se igualmente a realização de estudos longitudinais que permitam analisar a evolução da confiança dos utilizadores relativamente à utilização de plataformas digitais turísticas.

## 7.4 Considerações Finais

A transformação digital do setor do turismo representa uma oportunidade significativa para melhorar a experiência dos utilizadores e aumentar a competitividade das organizações turísticas. Contudo, a crescente utilização de dados pessoais em ambientes digitais torna essencial a integração de mecanismos adequados de privacidade e proteção de dados.

A presente investigação procurou contribuir para este contexto através do desenvolvimento e avaliação de uma aplicação turística digital orientada para a proteção de dados pessoais.

Os resultados obtidos demonstram que os utilizadores valorizam soluções digitais transparentes, confiáveis e centradas na proteção da privacidade.

Conclui-se, assim, que a integração de princípios de privacidade e proteção de dados constitui um elemento fundamental para o desenvolvimento sustentável e confiável do turismo digital em Cabo Verde.

Além do contributo académico, a investigação apresenta igualmente relevância prática, demonstrando que a proteção de dados pode ser incorporada como elemento estratégico no desenvolvimento de aplicações turísticas digitais.

Desta forma, espera-se que o presente estudo possa contribuir para futuras investigações relacionadas com turismo digital, privacidade, proteção de dados e desenvolvimento de soluções tecnológicas centradas no utilizador.

# REFERÊNCIA BIBLIOGRÁFICA

## Documentais e normativas


Decreto-Legislativo nº 133/V/2001, de 22 de janeiro – Lei de Proteção de Dados da República de Cabo Verde.

Decreto-Legislativo nº 41/VII/2013, de 17 de setembro - Altera o regime jurídico geral de proteção de dados pessoais das pessoas singulares, aprovado pela Lei nº 133/V/2001, de 22 de Janeiro.

Decreto-Legislativo nº 121/IX/2021, de 17 de março - Procede à segunda alteração do regime jurídico geral de proteção de dados pessoais das pessoas singulares aprovado pela Lei nº 133/V/2001, de 22 de janeiro, alterada pela Lei nº 41/VIII/2013, de 17 de setembro

Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados.

A Semana/InforPress. (2025). Agência Actour lança Cabo Verde no mapa digital mundial com o primeiro mapeamento nacional do Google Street View. Https://Www.Asemana.Cv/Atualidade/19089-Agencia-Actour-Lanca-Cabo-Verde%20no-Mapa-Digital-Mundial-Com-o-Primeiro-Mapeamento-Nacional-Do-Google-Street-View. https://www.asemana.cv/atualidade/19089-agencia-actour-lanca-cabo-verde%20no-mapa-digital-mundial-com-o-primeiro-mapeamento-nacional-do-google-street-view

Almeida, Germano., & Salvador, J. A. . (2003). Cabo Verde : viagem pela história das ilhas (2003 Editorial Caminho, Ed.). Editorial Caminho.

Barbosa, D. P., & Medaglia, J. (2020). Tecnologia digital, turismo e os hábitos de consumo dos viajantes contemporâneos. Marketing & Tourism Review, 4(2). https://doi.org/10.29149/mtr.v4i2.5394

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. IEEE Consumer Electronics Magazine, 9(2), 78–82. https://doi.org/10.1109/MCE.2019.2953739

Cejas, O. A., Sannier, N., Abualhaija, S., Ceci, M., & Bianculli, D. (2025). GDPR-Relevant Privacy Concerns in Mobile Apps Research: A Systematic Literature Review. http://arxiv.org/abs/2411.19142

Comitê Europeu para a Proteção de Dados. (2024). EDPB Annual Report 2023 SAFEGUARDING INDIVIDUALS' DIGITAL RIGHTS.

Elizabete, A., Enobe, C., Siqueira, L., & Junior, C. (2022). DESIGN SCIENCE RESEARCH-UM ESTUDO DE CASO SOBRE A PRÁTICA DE ENSINO DO MÉTODO EM ADMINISTRAÇÃO E GESTÃO DE PROJETOS.

ENISA, 2024. (2024). ENISA threat landscape 2024 : July 2023 to June 2024. ENISA.

European Union Agency for Fundamental Rights. (2023). Fundamental rights report 2023. Publications Office of the European Union.

Global Sustainable Tourism Council. (2023, June 30). Cabo Verde Gains GSTC-Recognized Status. Https://Www.Gstc.Org/Cabo-Verde-Gains-Gstc-Recognized-Status/.

Gómez-Goiri, A., Seco-Aguirre, I., Lage, O., & Ruiz, A. (2025). Privacy-preserving computation meets quantum computing: A scoping review. In Digital Communications and Networks (Vol. 11, Number 6, pp. 1707–1721). KeAi Communications Co. https://doi.org/10.1016/j.dcan.2025.05.010

Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: foundations and developments. Electronic Markets, 25(3), 179–188. https://doi.org/10.1007/s12525-015-0196-8

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. In Scandinavian Journal of Information Systems (Vol. 19, Number 2).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. In Design Science in IS Research MIS Quarterly (Vol. 28, Number 1).

Hoepman, J.-H. (2014). Privacy Design Strategies. https://doi.org/https://doi.org/10.1007/978-3-642-55415-5_38

Instituto do Turismo de Cabo Verde. (2018). Cabo Verde Is Something Else. Https://Turismo.Cv/Pt_PT/Page/Welcome-to-Cv.

Ioannou, A., Tussyadiah, I., & Miller, G. (2021). That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure. Journal of Travel Research, 60(7), 1510–1526. https://doi.org/10.1177/0047287520951642

Jakob Nielsen. (1994). Usability Engineering.

Kemp, S. (2025, March 3). Digital 2025: Cabo Verde. Https://Datareportal.Com/Reports/Digital-2025-Cabo-Verde. https://datareportal.com/reports/digital-2025-cabo-verde

Leithardt, V., Santos, D., Silva, L., Viel, F., Zeferino, C., & Silva, J. (2020). A Solution for Dynamic Management of User Profiles in IoT Environments. IEEE Latin America Transactions, 18(07), 1193–1199. https://doi.org/10.1109/TLA.2020.9099759

Madureira, J. S., & Schneider, H. N. (2025). DESIGN SCIENCE RESEARCH APLICADA A UMA PESQUISA EM EDUCAÇÃO: UM RELATO DE EXPERIÊNCIA Eixo 08-Metodologias da Pesquisa em Educação e Comunicação.

Michele Nogueira. (2025, May 2). A Computação Quântica e a Cibersegurança: O Futuro Promissor e Seus Desafios. Https://Horizontes.Sbc.Org.Br/Index.Php/2025/05/a-Computacao-Quantica-e-a-Ciberseguranca-o-Futuro-Promissor-e-Seus-Desafios/. https://horizontes.sbc.org.br/index.php/2025/05/a-computacao-quantica-e-a-ciberseguranca-o-futuro-promissor-e-seus-desafios/

Ministério das Finanças de Cabo Verde. (2025, November 21). Turismo é "setor estratégico e catalisador" do desenvolvimento de Cabo Verde, afirma Vice-Primeiro-Ministro, Olavo Correia, na Comissão Especializada. Https://Www.Mf.Gov.Cv/Web/Mf/-/Turismo-%C3%A9-Setor-Estrat%C3%A9gico-e-Catalisador-Do-Desenvolvimento-de-Cabo-Verde-Afirma-Vice-Primeiro-Ministro-Olavo-Correia-Na-Comiss%C3%A3o-Especializada.

Myers, M. D. (2020). QUALITATIVE RESEARCH in BUSINESS & MANAGEMENT THIRD EDITION.

Ordóñez-Martínez, D., Seguí-Pons, J. M., & Ruiz-Pérez, M. (2024). Conceptual Framework and Prospective Analysis of EU Tourism Data Spaces. Sustainability (Switzerland), 16(1). https://doi.org/10.3390/su16010371

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pimentel, M., Filippo, D., & Santoro, F. (2018). Design Science Research: fazendo pesquisas científicas rigorosas atreladas ao desenvolvimento de artefatos computacionais projetados para a educação.

Pires Silva Mendonça Orientação, C., & Barros Matos, J. (2018). UNIVERSIDADE DE ÉVORA ESCOLA DE ARTES DEPARTAMENTO DE ARQUITECTURA Arquitectura militar de Cabo Verde A Fortaleza Real de São Filipe e o sistema defensivo da Cidade Velha.

Powell, M. (2025). Privacy: Concept, Right, and Underlying Values. Philosophy and Technology, 38(3). https://doi.org/10.1007/s13347-025-00931-3

Preko, A., Sedalo, G., Zilevu, T. K., Yegblemenawo, C. A. A., Nimsaah, W. K., Kanda, W., & Yawson, G. M. (2025). International tourists' data privacy and destination referral: Ghana's perspective. SN Social Sciences, 5(4). https://doi.org/10.1007/s43545-025-01083-z

Rego Monteiro da Hora, H., Torres Rego Monteiro Professora Doutora da FioCruz, G., & Arica Professor Doutor da UENF, J. (2010). Confiabilidade em Questionários para Qualidade: Um Estudo com o Coeficiente Alfa de Cronbach (Vol. 11, Number 2).

Reis Quietinho Leithardt, V., Antonio Borges, G., Graciela de Morais Rossetto, A., Oberdan Rolim, C., Fernando Resin Geyer, C., Henrique Andrade Correia, L., Nunes, D., & Sa Silva, J. (2013). A Privacy Taxonomy for the Management of Ubiquitous Environments. In Journal of Communication and Computer (Vol. 10).

SGOBBI, L. F., BARBOSA, M. S., TELES, B. F., PAULA, D. S. de, & FERRI, P. H. (2024). WebCiência IQ-UFG: uma escala do tipo Likert na mensuração da opinião dos participantes. Revista ELO – Diálogos Em Extensão, 13. https://doi.org/10.21284/elo.v13i.17221

Silva, L. A., Leithardt, V. R. Q., Rolim, C. O., González, G. V., Geyer, C. F. R., & Silva, J. S. (2019). Priser: Managing notification in multiples devices with data privacy support. Sensors (Switzerland), 19(14). https://doi.org/10.3390/s19143098

Silveira, C., & Reis, L. (2022). Sustainability in Software Engineering: A Design Science Research Approach. 8th International Scientific ERAZ Conference – ERAZ 2022 – Conference Proceedings, 317–323. https://doi.org/10.31410/eraz.2022.317

Song, B., Pokhrel, S. R., Vasilakos, A. V., Zhu, T., & Li, G. (2025). Towards A Hybrid Quantum Differential Privacy. http://arxiv.org/abs/2501.07844

Sonja Lucic. (2023). Protection of personal data in the tourism sector - DOAJ. 11.

Unidade de Gestão de Projetos Especiais. (2023, May 9). Projeto Turismo Resiliente e Desenvolvimento da Economia Azul em Cabo Verde. Https://Ugpe.Gov.Cv/Projeto/Reforco-Da-Sustentabilidade-Resiliencia-e-Diversificacao-Do-Sector-Do-Turismo-Em-Cabo-Verde. https://ugpe.gov.cv/projeto/reforco-da-sustentabilidade-resiliencia-e-diversificacao-do-sector-do-turismo-em-cabo-verde

Yalcin, H., Daim, T., Moughari, M. M., & Mermoud, A. (2024). Supercomputers and quantum computing on the axis of cyber security. Technology in Society, 77. https://doi.org/10.1016/j.techsoc.2024.102556

Zhong, H., Ju, K., Shen, J., Zhang, X., Qin, X., Ohtsuki, T., Pan, M., & Han, Z. (2025). Differential Privacy Preserving Distributed Quantum Computing. http://arxiv.org/abs/2412.12387

# ANEXO

## Anexo A- Política de Privacidade

Esta Política de Privacidade descreve como a [GoCaboVerde] recolhe, utiliza, armazena e protege as informações pessoais dos seus utilizadores, de acordo com o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia e as boas práticas estabelecidas pela Comissão Nacional de Proteção de Dados de Cabo Verde.

**1. Responsável pelo tratamento**

Na [GoCaboVerde], entendemos a importância da privacidade e estamos comprometidos em proteger as informações pessoais dos nossos utilizadores. A nossa Política de Privacidade visa esclarecer como tratamos os dados pessoais recolhidos e quais são os direitos que os utilizadores podem exercer.

Contacto geral: [heniol@gmail.com] | [+238 1234567]

Morada: [Palmarejo]

Encarregado de Proteção de Dados ("DPO"): [EMAIL DPO – caso não tenham email empresa]

**2. Dados Pessoais recolhidos**

Recolhemos as seguintes informações pessoais quando os utilizadores se registam na nossa plataforma ou interagem com os nossos serviços:

- Informações de Identificação: nome, endereço de e-mail, número de telefone, e data de nascimento.
- Informações de Localização: dados de localização, como cidade ou região.
- Informações de Preferências: preferências turísticas, como pontos turísticos favoritos, eventos de interesse e serviços adicionais preferidos.
- Dados de Acesso: informações de login, como nome de utilizador e senha.

**3. Finalidade de Tratamento**

Os dados pessoais que recolhemos são utilizados para as seguintes finalidades:

- Personalizar a experiência do utilizador, oferecendo recomendações de serviços e pontos turísticos com base nas suas preferências.
- Enviar comunicações promocionais e informações sobre eventos ou ofertas que possam ser do interesse do utilizador.
- Garantir a segurança da nossa plataforma e prevenir atividades fraudulentas.
- Cumprir com obrigações legais e regulatórias, como a legislação de proteção de dados.

**4. Base Legal para o Tratamento de Dados**

A base legal para o tratamento dos dados pessoais dos utilizadores é:

- Consentimento: Ao aceitar esta Política de Privacidade, o utilizador consente a recolha e o tratamento dos seus dados pessoais conforme descrito.
- Execução de Contrato: O tratamento de dados é necessário para a prestação dos serviços oferecidos pela nossa plataforma.
- Cumprimento de Obrigações Legais: O tratamento de dados pode ser necessário para cumprir com exigências legais ou regulatórias.

**5. Retenção de Dados**

Os dados pessoais serão conservados apenas pelo tempo necessário para cumprir com as finalidades descritas nesta Política de Privacidade, ou conforme exigido por lei. Após o término do período de retenção, os dados serão eliminados de forma segura.

**6. Direitos dos Titulares dos Dados**

Os utilizadores têm os seguintes direitos em relação aos seus dados pessoais:

- Acesso: Direito de aceder aos seus dados pessoais e obter informações sobre como são tratados.
- Retificação: Direito de corrigir dados pessoais incorretos ou incompletos.
- Eliminação: Direito de solicitar a eliminação dos dados pessoais quando não forem mais necessários para as finalidades para as quais foram recolhidos.
- Portabilidade: Direito de receber os dados pessoais que nos forneceu num formato estruturado e de fácil leitura, ou de os transferir para outro controlador.
- Oposição: Direito de se opor ao tratamento dos seus dados pessoais em determinadas circunstâncias, especialmente no caso de tratamentos para marketing direto.
- Limitação do Tratamento: Direito de solicitar a limitação do tratamento dos seus dados pessoais em algumas situações específicas.

**7. Proteção dos Dados Pessoais**

Adotamos medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, divulgação, alteração ou destruição.

**8. Partilha de Dados Pessoais**

Não partilhamos os dados pessoais dos utilizadores com terceiros, exceto quando:

- É necessário para a prestação dos serviços, como parceiros de transporte ou fornecedores de serviços turísticos.

- A partilha é exigida por lei ou para proteger os direitos, propriedade ou segurança dos utilizadores.

**9. Transferências Internacionais de Dados**

Os dados pessoais podem ser transferidos para fora do Espaço Económico Europeu (EEE) para países que não oferecem o mesmo nível de proteção de dados. Nesses casos, garantimos que os dados são tratados de acordo com os princípios do RGPD, utilizando mecanismos legais adequados para proteger a privacidade dos utilizadores.

**10. Recolha de Cookies e Outras Tecnologias de Monitorização**

Esta aplicação utiliza cookies para melhorar a experiência do utilizador, personalizar conteúdo e anúncios, fornecer funcionalidades de redes sociais e analisar o tráfego do site. Os cookies são pequenos ficheiros de dados armazenados no seu dispositivo que ajudam a reconhecer as suas preferências e a melhorar a navegação. O utilizador tem o direito de alterar as definições dos cookies a qualquer momento, podendo, se assim o desejar, desativar ou configurar os cookies nas definições do seu navegador. No entanto, a desativação de cookies pode afetar a funcionalidade de certas áreas do site ou da aplicação. Para uma gestão mais detalhada dos cookies, incluindo a visualização das suas categorias e finalidades, o utilizador pode aceder à gestão de cookies, disponível na página de configurações de privacidade.

**11. Privacy by Design e Privacy by Default**

A privacidade é incorporada em nosso sistema desde a sua concepção, de acordo com os princípios de *Privacy by Design* e *Privacy by Default*. Isso significa que garantimos que apenas os dados necessários para as finalidades do serviço sejam recolhidos e processados, e que a segurança e a proteção da privacidade sejam consideradas em todas as fases do desenvolvimento e operação da nossa plataforma.

**12. Alterações à Política de Privacidade**

Podemos atualizar esta Política de Privacidade de tempos em tempos para refletir alterações nas nossas práticas de privacidade ou nas exigências legais. Quaisquer alterações serão publicadas nesta página com a data da última atualização.

**13. Contacto**

Se tiver alguma dúvida sobre esta Política de Privacidade ou sobre como tratamos os seus dados pessoais, pode entrar em contacto connosco através do seguinte endereço de e-mail: [heniol@gmail.com].

**Versão:** 1.0

**Data de entrada em vigor:** [dd/mm/aaaa]

## Anexo B Questionário

Exmo.(a). Senhor (a) Turista

O presente questionário insere-se num projeto de investigação que estamos a desenvolver no âmbito da dissertação do ciclo de estudos de Mestrado em Informática e Gestão do ISCTE – Instituto Universitário de Lisboa em Portugal, relacionada com privacidade, proteção de dados e turismo digital em Cabo Verde.

Este questionário será aplicado aos turistas com o objetivo de avaliarem o protótipo turístico desenvolvido com foco em mecanismos de privacidade e proteção de dados pessoais, referindo que às questões apresentadas, não existirão respostas corretas ou incorretas. Solicitamos e agradecemos que as respostas sejam espontâneas e sinceras, pois o que vale mesmo é a sua opinião.

Os resultados são confidenciais, sendo empregues apenas para os fins apontados.

Muito obrigado pela sua colaboração.

### PARTE I – IDENTIFICAÇÃO PESSOAL

**Idade**

- 18 a 24 anos
- 25 a 30 anos
- 36 a 40 anos
- 41 a 50 anos
- 55 ou mais

**Género**

- Feminino
- Masculino
- Prefiro não responder
- Outro

**Habilitações Académicas**

- Ensino secundário
- Licenciatura
- Pós-graduação
- Mestrado
- Doutorado
- Outro

### PARTE B – PERCEÇÃO SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

| | Discordo totalmente | Discordo | Nem concordo nem discordo | Concordo | Concordo totalmente |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| B1. Considero importante que aplicações turísticas protejam os dados pessoais dos utilizadores. | | | | | |
| B2. Costumo preocupar-me com a forma como os meus dados pessoais são utilizados em plataformas digitais. | | | | | |
| B3. Sinto maior confiança em aplicações que apresentam informações claras sobre privacidade. | | | | | |
| B4. O consentimento para recolha de dados deve ser apresentado de forma clara e transparente. | | | | | |
| B5. Os utilizadores devem ter controlo sobre os seus dados pessoais em aplicações digitais. | | | | | |

**PARTE C – AVALIAÇÃO DO PROTÓTIPO**

| | Discordo totalmente | Discordo | Nem concordo nem discordo | Concordo | Concordo totalmente |
|---|---|---|---|---|---|
| | | | | | |
| AP1. O protótipo foi fácil de utilizar. | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| AP2. A navegação na aplicação foi clara e intuitiva. | | | | | |
| AP3. As funcionalidades disponíveis foram fáceis de compreender. | | | | | |
| AP4. O sistema apresentou informações claras sobre o tratamento dos dados pessoais. | | | | | |
| AP5. As opções relacionadas com privacidade estavam facilmente visíveis. | | | | | |
| AP6. Consegui compreender quais dados pessoais seriam recolhidos. | | | | | |
| AP7. O sistema transmitiu confiança durante a utilização. | | | | | |
| AP8. O protótipo aparenta respeitar princípios de privacidade e proteção de dados. | | | | | |
| AP9. Senti que possuía controlo sobre os meus dados pessoais durante a utilização. | | | | | |
| AP10. A utilização da aplicação aumentaria a minha confiança em serviços digitais de turismo. | | | | | |
| AP11. Utilizaria uma | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| aplicação semelhante num contexto real. | | | | | |

## PARTE D – AVALIAÇÃO GLOBAL DA SOLUÇÃO

| | Muito inadequado | Inadequado | Nem Adequado nem inadequado | Adequado | Muito adequado |
|---|---|---|---|---|---|
| AG1. Clareza das informações sobre recolha de dados. | | | | | |
| AG2. Transparência sobre utilização dos dados pessoais. | | | | | |
| AG3. Facilidade de gestão do consentimento. | | | | | |
| AG4. Perceção de segurança dos dados pessoais. | | | | | |
| AG5. Proteção da privacidade durante a utilização da aplicação. | | | | | |
| AG6. Confiança geral transmitida pela solução. | | | | | |

## PARTE E – QUESTÕES ABERTAS

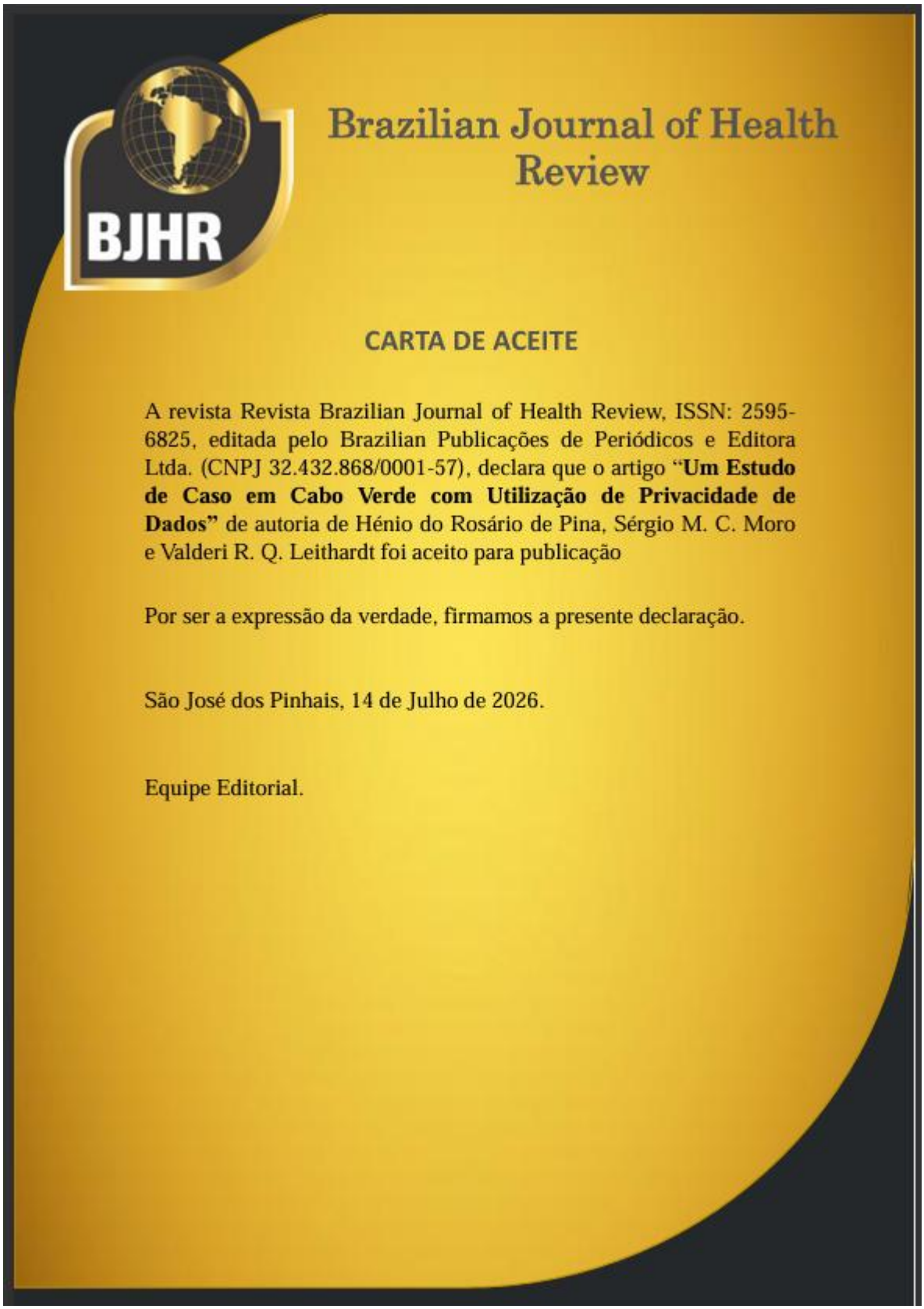
QA1. Quais foram os aspetos mais positivos da aplicação?

QA2. Quais aspetos poderiam ser melhorados?

QA3. Considera que esta aplicação pode contribuir para melhorar a privacidade e proteção de dados no turismo digital? Justifique.

QA4. Sugestões ou comentários adicionais

**Anexo C – Carta de Aceite**



Brazilian Journal of Health Review

CARTA DE ACEITE

A revista Revista Brazilian Journal of Health Review, ISSN: 2595-6825, editada pelo Brazilian Publicações de Periódicos e Editora Ltda. (CNPJ 32.432.868/0001-57), declara que o artigo "**Um Estudo de Caso em Cabo Verde com Utilização de Privacidade de Dados"** de autoria de Hénio do Rosário de Pina, Sérgio M. C. Moro e Valderi R. Q. Leithardt foi aceito para publicação

Por ser a expressão da verdade, firmamos a presente declaração.

São José dos Pinhais, 14 de Julho de 2026.

Equipe Editorial.