INSTITUTO SUPERIOR POLITÉCNICO DE CIÊNCIAS E TECNOLOGIA

CURSO DE ENGENHARIA INFORMÁTICA E SISTEMAS DE INFORMAÇÃO

A Criação de um *Website* para Denúncia de Burla em Angola, no Ano de 2026

Autor: Ivânio Manuel Quiosa

Orientador: Pedro Nascimento

Luanda – 2026

INSUTEC
INSTITUTO SUPERIOR POLITÉCNICO
DE CIÊNCIAS E TECNOLOGIA

DECLARAÇÃO DE APROVAÇÃO DO ORIENTADOR

Eu, Pedro Nascimento na qualidade de orientador, certifico que o presente trabalho atende os requisitos académicos, científicos e metodológicos exigidos pela instituição, reflectindo um esforço genuíno do estudante na investigação e na produção do conhecimento.

Assim, considero que o trabalho está apto para a sua apresentação e avaliação pela banca examinadora.

Luanda, aos_____de_____de 20_____

_____

Assinatura do Orientador

INSTITUTO SUPERIOR POLITÉCNICO DE CIÊNCIAS E TECNOLOGIA

CURSO DE ENGENHARIA INFORMÁTICA E SISTEMAS DE INFORMAÇÃO

A Criação de um *Website* para Denúncia de Burla em Angola, no Ano de 2026

Autor: Ivânio Manuel Quiosa

Orientador: MsC. Pedro Nascimento

Luanda – 2026

TERMO DE APROVAÇÃO

Eu, Ivânio Manuel Quiosa, certifico que este trabalho é original_____

Tema: A Criação de um *Website* para Denúncia de Burla em Angola, no Ano de 2026

"Trabalho de Conclusão de Curso apresentado ao Instituto Superior Politécnico de Ciências e Tecnologia como parte dos requisitos para obtenção do grau académico de Licenciatura em Engenharia Informática e Sistemas de Informação."

Esta Monografia foi avaliada e aprovada para obtenção do título de licenciado no curso de Engenharia Informática e Sistemas de Informação.

_____

Mestre prof. Pedro Nascimento
Orientador

_____

Mestre prof. Rouget Ruano
Presidente do Júri

_____

Mestre prof. Irene Monier
Arguente

_____

Licenciado prof. Álvaro Jorge
Arguente

Luanda – 2026

DEDICATÓRIAS

Dedico este trabalho primeiramente a Deus, por me conceder força e sabedoria durante toda esta caminhada.

À minha família, pelo apoio incondicional, amor e compreensão nos momentos de ausência.

Aos meus amigos e colegas, que sempre estiveram presentes compartilhando alegria e desafio.

E a todos que, de alguma forma, contribuíram para que este sonho se tornasse realidade.

AGRADECIMENTOS

Agradeço primeiramente a Deus, fonte de inspiração e perseverança, por ter me guiado até aqui.

Aos meus pais e familiares, pela paciência, incentivo e carinho em todos os momentos desta jornada.

Ao meu orientador, “Pedro Nascimento”, pela dedicação, orientação, ensinamentos e por acreditar no meu potencial.

Aos professores e colegas do curso, pelas trocas de experiências e pelo convívio enriquecedor ao longo desta trajectória académica.

Aos amigos que me acompanharam nesta caminhada, pela amizade, apoio e motivação.

E, por fim, agradeço a todos que, directa ou indirectamente, contribuíram para a realização deste trabalho.

RESUMO

O presente trabalho aborda o fenómeno da burla em Angola, analisando sua ocorrência em diferentes contextos e propondo como solução a criação do *website* StopBurla para registo e acompanhamento de denúncias. A pesquisa parte da constatação da escassez de canais digitais confiáveis que auxiliam cidadãos na identificação, prevenção e denúncia de práticas fraudulentas, comprometendo a segurança digital e a confiança social. O objectivo geral é criar o *website* StopBurla para denúncia de burla em Angola. Foram definidos objectivos específicos relacionados à análise do fenómeno, levantamento de requisitos, desenvolvimento de protótipos e avaliação do contributo da ferramenta para o fortalecimento da cidadania digital. Metodologicamente, trata-se de uma investigação aplicada, descritiva e de abordagem qualitativa, orientada por métodos dedutivo-indutivo, análise-síntese e hipotético-dedutivo, complementados por procedimentos empíricos de observação directa e modelagem. A criação do *website* StopBurla baseou-se na utilização de tecnologias *web*, diagramas UML e protótipos visuais, possibilitando a validação prévia da sua estrutura lógica e funcional. O estudo revela a importância de ferramentas digitais na prevenção e no combate à burla, evidenciando a relevância da integração entre tecnologia, cidadania e segurança digital para o contexto angolano.

Palavras-chave: Angola; Burla; Cidadania Digital; Segurança; *Website*.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÓNIMOS E SIGLAS

APA – *American psychological association* (Associação americana de psicologia)

BR – Burla

CSS – *Cascading style sheets* (Folhas de estilo em cascata)

DII – Desenvolvimento iteractivo e incremental

ER – Entidade-relacionamento

FCA – Faculdade de Ciências e Tecnologia

FK – Chave estrangeira

GDPR – General data *protection regulation* (Regulamento geral de protecção de dados)

HTML – *HyperText markup language* (Linguagem de marcação de hipertexto)

HTTPS – *HyperText transfer protocol secure* (Protocolo de transferência de hipertexto seguro)

IA – Inteligência artificial

IPS – *Intrusion prevention system* (Sistema de prevenção de intrusão)

JS – *JavaScript*

JSON – *JavaScript object notation* (Notação de objecto *javaScript*)

ONU – Organização das nações unidas

PHP – *Hypertext* preprocessor (Pré-processador de hipertexto)

PDF – *Portable document format* (Formato de documento portátil)

PWC – *PricewaterhouseCoopers*

PK – Chave primária

RN – Requisitos funcionais

RNF – Requisitos não funcionais

SQL – *Structured query language* (Linguagem de consulta estruturada)

UC – *Use case* (Caso de uso)

UML – *Unified modeling language* (Linguagem de modelagem unificada)

UE – União europeia

VS – Visual *studio*

WEB – *World Wide Web* (Rede mundial de computadores)

WCAG – *Web content accessibility guidelines* (Directrizes de acessibilidade de conteúdo da *web*)

XAMPP – *Cross-Platform*, Apache, MariaDB/*MySQL*, PHP, *Perl*

LISTA DE SÍMBOLO

% – Por cento

INTRODUÇÃO

A burla, nas suas múltiplas formas, constitui um problema global que acompanha a evolução das tecnologias de comunicação e da economia digital. Em diversos países, este fenómeno tem provocado sérios prejuízos financeiros e sociais, afectando indivíduos, empresas e até mesmo instituições públicas. A crescente sofisticação dos métodos utilizados pelos burladores, aliada à facilidade de acesso à *internet*, tem desafiado sistemas de segurança e exigido respostas cada vez mais eficazes no combate a tais práticas.

No contexto africano, e particularmente em Angola, a problemática da burla assume proporções preocupantes. A expansão do uso das redes sociais e do comércio electrónico, somada pela literacia digital da população, tem contribuído para a vulnerabilidade de muitos cidadãos. Casos recorrentes de burlas, desde falsos anúncios de emprego e vendas fraudulentas até esquemas financeiros duvidosos, revelam a necessidade urgente de mecanismos que possam denunciar e prevenir tais situações.

A nível local, a ausência de plataformas digitais específicas para denúncia de burlas representa uma lacuna no processo de protecção da sociedade. Muitas vítimas não sabem a quem recorrer ou, por receio de represálias e desconfiança nas instituições, acabam silenciando os casos sofridos. Este cenário favorece a continuidade das práticas ilícitas e fragiliza a confiança nas interacções sociais e comerciais, tanto presenciais quanto virtuais.

Diante desta realidade, a criação do *website* StopBurla em Angola apresenta-se como uma proposta relevante e necessária. Tal iniciativa visa não apenas oferecer um canal seguro e acessível para os cidadãos reportarem ocorrências, mas também fomentar sobre o problema, apoiar investigações e contribuir para a construção de um ambiente digital mais confiável. Assim, este trabalho justifica-se pela pertinência social, tecnológica e académica de desenvolver soluções inovadoras voltadas para a protecção da comunidade angolana.

Problematização

A burla, enquanto prática ilícita, é um fenómeno em constante crescimento que acompanha a evolução tecnológica e os novos meios de comunicação. Actualmente, o ambiente digital tem servido de palco privilegiado para a proliferação de esquemas fraudulentos, os quais exploram a vulnerabilidade e a falta de literacia digital de grande parte da população. Esta realidade tem gerado consequências significativas, desde perdas financeiras até danos psicológicos e sociais, comprometendo a confiança dos cidadãos no uso das plataformas digitais.

Em Angola, o problema da burla ganha contornos ainda mais complexos devido à ausência de canais especializados que permitem o registo e a denúncia eficaz desses casos. Apesar do aumento das ocorrências em redes sociais, no comércio informal e em transações electrónicas, as vítimas enfrentam dificuldades em denunciar por medo de represálias, desconhecimento sobre os órgãos competentes ou simplesmente pela inexistência de um espaço acessível e confiável que centraliza tais denúncias. Essa lacuna institucional favorece a continuidade e o aperfeiçoamento das práticas fraudulentas.

Adicionalmente, observa-se que as iniciativas existentes para combater a burla ainda são limitadas, pouco divulgadas ou de difícil acesso para a população em geral. A carência de plataformas digitais específicas fragiliza os mecanismos de prevenção e investigação, resultando numa subnotificação significativa dos casos. Este cenário revela uma necessidade urgente de desenvolver soluções tecnológicas inovadoras que possibilitam às vítimas reportar situações de forma segura e que contribuem para a construção de um ambiente social e digital mais protegido.

Pergunta de partida

Como a criação do *website* StopBurla pode contribuir para a redução deste fenómeno e para a promoção de maior segurança digital em Angola?

Hipótese

A criação do *website* StopBurla em Angola contribuirá para a redução do fenómeno, ao oferecer um canal acessível, seguro e confiável para o registo de ocorrências, permitindo maior visibilidade dos casos, apoio às autoridades competentes sobre os riscos das práticas fraudulentas.

Objectivo geral

- Criar um *Website* para Denúncia de Burla em Angola.

Objectivos específicos

- Analisar o fenómeno da burla em nível global, nacional e local, identificando suas principais formas de ocorrência e impacto na sociedade angolana.
- Levantar os requisitos funcionais e não funcionais necessários para a criação do *website* StopBurla seguro, acessível e eficaz no registo de denúncias de burla.

- Projectar um protótipo funcional do *website* StopBurla, integrando recursos que permitem o registo de denúncias, consulta de informações e acesso a orientações preventivas.
- Avaliar a contribuição do *website* StopBurla para o fortalecimento da segurança digital em Angola, propondo melhorias futuras.

Delimitação

Esta pesquisa foi desenvolvida no ano de 2025, no contexto da realidade social e tecnológica de Angola, com foco na análise do fenómeno da burla no ambiente digital. O estudo limitou-se no desenvolvimento do *website* StopBurla, abrangendo o levantamento de requisitos e construção do protótipo.

Justificativa

A escolha deste tema justifica-se, em primeiro lugar, pela relevância social do combate à burla em Angola. Este fenómeno, que afecta diariamente cidadãos e instituições, provoca perdas financeiras significativas e fragiliza a confiança nas interacções sociais e digitais. Ao propor a criação do *website* StopBurla, busca-se contribuir para a protecção da população e para a promoção de uma cultura de segurança digital mais sólida e consciente.

Em segundo lugar, a pesquisa apresenta novidade ao propor uma solução tecnológica direccionada especificamente ao contexto angolano. Apesar da crescente digitalização dos serviços, ainda não existem plataformas digitais especializadas que centralizam denúncias de burla e oferecem informações preventivas de forma acessível. Assim, o projecto responde a uma lacuna concreta e propõe um instrumento inovador, alinhado com as necessidades actuais da sociedade.

Por fim, a pertinência académica e tecnológica do estudo reside no facto de unir a prática investigativa com a aplicação real de conhecimentos adquiridos ao longo da formação. O desenvolvimento do *website* StopBurla como ferramenta de denúncia não só fortalece a relação entre teoria e prática, como também amplia o campo de possibilidades de pesquisa em segurança digital, tecnologia da informação e cidadania digital em Angola.

Metodologia

Classificação da pesquisa

- Quanto à natureza: esta pesquisa é aplicada, pois visa o desenvolvimento do *website* StopBurla prático e funcional voltado para denúncia de burlas no contexto angolano. O estudo busca a resolução de um problema concreto e actual, que é a falta de canais digitais confiáveis para denúncia, implementando uma solução tecnológica que fortalece a segurança digital e apoia a sociedade na prevenção de fraudes.
- Quanto aos objectivos: classifica-se como uma pesquisa descritiva, uma vez que procura identificar, organizar e apresentar informações relevantes sobre a ocorrência de burlas em Angola, assim como descrever os requisitos técnicos e funcionais necessários para o correcto desenvolvimento do *website* StopBurla.
- Segundo a abordagem do problema**:** a investigação adopta uma abordagem qualitativa, uma vez que se orienta para a descrição e compreensão das funcionalidades, estrutura e características do *website* StopBurla para o apoio ao combate à burla. Essa abordagem permite analisar, de forma detalhada, os requisitos do sistema, a organização da informação, a usabilidade e a interacção com os utilizadores, considerando documentos institucionais, necessidades identificadas e percepções dos potenciais utilizadores, sem recorrer a métodos estatísticos de tratamento de dados.

Métodos de nível teórico ou de abordagem

- Dedutivo-indutivo: a investigação parte de conceitos gerais sobre segurança digital, usabilidade e desenvolvimento do *website* StopBurla, aplicando-os ao contexto angolano de combate à burla. Ao final, os resultados obtidos são analisados para verificar se os pressupostos teóricos se confirmam na prática.
- Análise-síntese: inicialmente, as informações recolhidas foram analisadas isoladamente, identificando os principais problemas enfrentados pelas vítimas de burla. Posteriormente, esses dados foram integrados para definir os requisitos técnicos e funcionais do *website* StopBurla.
- Hipotético-dedutivo: a pesquisa formula a hipótese de que a criação do *website* StopBurla contribuirá para a prevenção e a redução do fenómeno. Essa hipótese é verificada através do desenvolvimento e da validação do protótipo junto a potenciais utilizadores.

Métodos de nível empírico ou de procedimentos

- Observação directa: através da observação directa e análise do comportamento social dos cidadãos, foi possível identificar as formas mais comuns de burla em Angola, os meios habitualmente utilizados pelos burladores e o nível de conhecimento da população sobre medidas de prevenção. Essa observação permitiu compreender as percepções colectivas sobre o fenómeno, reconhecer os principais tipos de fraude recorrentes e detectar fragilidades na comunicação e sensibilização pública. As informações recolhidas serviram de base para definir as funcionalidades essenciais do *website*, garantindo que o sistema respondesse de forma eficaz às necessidades reais da sociedade.
- Modelagem: foram utilizados diagramas UML (Casos de Uso, Classes, Sequências e Actividades) e protótipos visuais para representar a estrutura lógica e funcional do *website* StopBurla.

Estrutura da monografia

O presente trabalho está organizado da seguinte forma:

- Introdução

Apresenta o tema da pesquisa, a delimitação do problema, a justificativa, a pergunta de partida, a hipótese, o objectivo geral e os objectivos específicos, bem como a metodologia adoptada. Esta secção contextualiza a relevância do estudo e introduz a proposta de criação do *website* StopBurla.

- Capítulo I – Fundamentação teórica

Discute os principais conceitos relacionados à burla e seus impactos sociais, jurídicos e digitais. São abordados temas como segurança da informação, cibercrime, cidadania digital, usabilidade de *websites*, acessibilidade, anonimato em denúncias *online* e metodologias ágeis de desenvolvimento de *software*.

- Capítulo II – Apresentação do *website* StopBurla

Apresenta as etapas práticas da criação do *website* StopBurla, desde o levantamento de requisitos até a implementação das funcionalidades. Inclui a modelagem com diagramas UML (casos de uso, classes, sequências e actividades), a arquitectura da base de dados, o *design* da *interface* e os testes de segurança e usabilidade. Também descreve as ferramentas utilizadas, os desafios enfrentados e as soluções adoptadas.

- Conclusão

Apresenta uma síntese dos resultados alcançados, confrontando-os com os objectivos e a hipótese formulada. Expõe as contribuições do trabalho para a sociedade e para a segurança digital em Angola, além de indicar limitações da pesquisa e sugestões para futuros estudos.

- Referências

Lista todas as fontes consultadas (livros, artigos científicos, relatórios, legislações e *sites* institucionais), organizadas segundo as normas da APA (7ª edição).

- Apêndices

Contém materiais complementares, como protótipos de tela, diagramas UML, capturas do *website* StopBurla, documentação técnica e a estrutura detalhada da base de dados.

CAPÍTULO I – FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, será abordada a fundamentação teórica que sustenta o desenvolvimento do presente trabalho, apresentando os principais conceitos, princípios e estudos relacionados ao tema. Serão discutidos aspectos teóricos sobre *websites*, bem como as tecnologias envolvidas no processo de criação.

1.1 Antecedentes históricos e contextualização da burla

1.1.1 Origem e evolução das práticas de burla no mundo

De acordo com Schulz (2007), já no Direito Romano se registavam práticas que envolviam engano deliberado para obter vantagem patrimonial, o que, embora não fosse chamado "burla" no sentido moderno, continha os elementos essenciais de manipulação e fraude (p. 112). Schulz mostra que essas práticas muitas vezes serviam de falsas declarações ou dissimulações, espelhando aquilo que mais tarde veio a ser tipificado como artifícios fraudulentos. Dessa forma, a burla tem raízes profundas nos sistemas jurídicos antigos, indicando que sua evolução está ligada ao desenvolvimento da noção de propriedade, confiança e dever legal de honestidade.

Avançando para a Idade Média e os tempos modernos, autores como Brandt (2007) ressaltam que as legislações germânicas e o direito canônico introduziram distinções entre engano moral e material, refinando os critérios do que seria considerado burla, incluindo a distinção entre dolo e culpa (p. 45). Brandt observa que essas distinções prepararam o terreno para que, nos séculos XVIII e XIX, com o surgimento do direito penal codificado na Europa, se formassem conceitos legais mais sistemáticos de burla. Em particular, o Código Napoleônico (1804) serviu de base para muitas codificações posteriores que definiram "fraude" como o uso de artifícios para provocar erro na vítima, com prejuízo patrimonial.

Mais adiante, Pinto (2008) argumenta que a modernização das comunicações e do comércio global, bem como a emergência da sociedade da informação, provocou uma mudança qualitativa nas práticas fraudulentas, ampliando tanto os métodos como os agentes envolvidos (p. 29). Segundo Pinto, o advento de transações electrónicas e redes digitais expandiu o universo das burlas, tornando-as mais complexas, internacionais e difíceis de rastrear. Assim, a burla evoluiu de pequenos golpes locais para esquemas institucionais, exigindo novas respostas legais e regulatórias.

1.1.2 A burla no contexto africano

Segundo Mbiti (2007), práticas culturais tradicionais de troca e confiança, combinadas com estruturas governamentais frágeis, criaram espaços propícios para burlas em diversas sociedades africanas, onde a verificação formal de identidade ou propriedade nem sempre existia (p. 78).

Mbiti destaca que essas práticas não eram vistas originalmente como crimes, mas como desordens sociais, até que o colonialismo impôs normas legais externas que reinterpretaram muitos actos de engano como ilícitos. Tal processo alterou profundamente como burlas eram julgadas, tanto social quanto legalmente.

Ademais, Nnoli (2003) nota que, após a independência, muitos estados africanos enfrentaram desafios económicos e institucionais, inflacção, desemprego elevado, burocracia ineficiente que proporcionaram incentivos para a prática de burlas, inclusive por funcionários públicos, para complementar rendimentos ou sobreviver (p. 104). Nnoli aponta que em muitos casos a impunidade ou a falta de capacidade de fiscalização fortaleceu essas práticas, tornando-as rotineiras e embutidas no funcionamento cotidiano das instituições. Para ele, a fraude passa a ser tanto um sintoma como um agravante da fragilidade institucional.

Mais recentemente, Kimani & Wanjiku (2017) afirmam que com a expansão do uso de tecnologia móvel, serviços financeiros digitais e comércio electrónico, surgiram novas formas de burla no continente africano, como fraudes tipo "419" por *email*, golpes de *mobile money*, *phishing* e falsificação digital que aproveitam lacunas na regulamentação e na literacia digital (p. 215). Esses autores enfatizam que, ao mesmo tempo em que há um grande potencial de crescimento tecnológico, existe um grande risco de vulnerabilidade para populações pouco acostumadas a lidar com tecnologia, o que amplia o impacto social dessas burlas.

1.1.3 Cenário actual da burla em Angola

De acordo com o relatório da PwC (2018), "Angola: *Economic* Crime *and Fraud Survey*", 64% das fraudes nas organizações angolanas são cometidas por agentes internos, indicando uma significativa vulnerabilidade institucional doméstica (p. 32). O estudo aponta que essas fraudes internas têm impacto directo não apenas financeiro, mas também reputacional, afectando a confiança nas instituições bancárias, empresariais e no sector público. Assim, a burla em Angola não é apenas externa, mas muitas vezes enraizada no funcionamento interno das próprias organizações.

Em um trabalho de auditoria interna recente, Silva et al. (2020) evidenciam que instituições bancárias angolanas enfrentam desafios estruturais na prevenção da fraude, como controlos internos frágeis, ausência de sistemas de rastreamento de transações suspeitas e falta de pessoal capacitado em *compliance* (p. 57). Segundo Silva et al., esses factores dificultam muito a detecção precoce de burlas e agravam as perdas patrimoniais, sobretudo em casos de fraude digital e burla combinada com lavagem de dinheiro.

Por fim, Quintino (2018), no estudo "A fraude fiscal e os crimes afins em Angola", refere que as normas tributárias e penais relativas à burla e ao abuso de confiança fiscal têm passado por reformas para responder aos novos tipos de fraude, inclusive exigindo notificações prévias, limites mínimos de valores e maior clareza no dever de comprovação do dolo (p. 14). Contudo, Quintino alerta que a aplicação prática dessas normas ainda enfrenta entraves, como sobrecarga dos tribunais, corrupção, e dificuldade de acesso à justiça por parte de vítimas de menor poder económico.

1.2 Conceitos fundamentais

1.2.1 Definição de burla (jurídica, social e digital)

Segundo Fragoso (2012), no campo jurídico a burla é definida como "o acto pelo qual um agente, mediante artifício ou engano, induz outrem no erro, obtendo vantagem ilícita em prejuízo patrimonial da vítima" (p. 91). Esta concepção centra-se no dolo e na intenção do agente, sendo fundamental para a tipificação penal e a delimitação entre ilícito civil e penal. Assim, o conceito jurídico estabelece a burla como crime contra o património, dependente do dolo e prejuízo efectivo.

Já sob a óptica social, Almeida (2016) entende que a burla não se resume ao ilícito penal, mas configura uma prática que corrói os laços de confiança na sociedade, minando a solidariedade e a cooperação (p. 47). Para o autor, ao disseminar desconfiança generalizada, a burla cria uma cultura de suspeita, prejudicando as relações de vizinhança, de comércio e até as interacções interpessoais. Desta forma, a burla é vista como fenómeno social que ultrapassa os limites jurídicos.

No ambiente digital, Costa & Ramos (2020) definem a burla como qualquer manipulação tecnológica que engana a vítima, explorando vulnerabilidades em sistemas digitais para apropriação ilícita de recursos (p. 133).

Neste sentido, golpes via *email*, *phishing*, clonagem de cartões e burlas em plataformas de *mobile banking* são manifestações contemporâneas de um mesmo fenómeno de engano fraudulento. A burla digital, portanto, amplia a abrangência do conceito para além da interacção presencial, incluindo mecanismos virtuais.

1.2.2 Diferenças entre burla, fraude e cibercrime

De acordo com Tavares (2011), a burla é juridicamente uma forma de fraude específica, em que o engano induzido leva a vítima a praticar actos de disposição patrimonial em prejuízo próprio (p. 76). Já fraude é um conceito mais amplo, podendo envolver falsificação documental, manipulação contábil ou outras práticas que não se enquadram necessariamente na tipificação de burla. Assim, toda burla é fraude, mas nem toda fraude é burla.

Segundo Gomes (2017), o cibercrime representa um campo mais vasto, englobando tanto a burla digital como outros ilícitos praticados por meio da tecnologia da informação, como invasão de sistemas, espionagem digital e disseminação de *malware* (p. 122). Para ele, a burla no ciber-espaço é apenas uma das tipologias dentro do fenómeno maior do cibercrime, que tem repercussões transnacionais. A distinção é essencial para a persecução penal e a formulação de políticas públicas de segurança digital.

Em contrapartida, Oliveira (2019) defende que, embora os três conceitos tenham pontos de intersecção, é necessário distingui-los com clareza para não fragilizar a aplicação da lei (p. 89). O autor argumenta que confundir burla com fraude ou cibercrime pode levar a erros na tipificação legal e prejudicar a protecção da vítima. Por isso, a clareza conceitual é não apenas teórica, mas prática, para os operadores do direito e as instituições de prevenção e combate.

1.2.3 Impactos sociais, económicos e psicológicos da burla

Conforme Silva (2015), os impactos sociais da burla manifestam-se na erosão da confiança social, no aumento da percepção de insegurança e no fortalecimento de redes ilícitas que competem com estruturas legítimas de mercado (p. 58). Essa degradação afecta especialmente países em desenvolvimento, onde o capital social é um recurso vital para a coesão comunitária. A burla, assim, compromete a solidariedade e favorece práticas de individualismo predatório.

No campo económico, Pinto & Carvalho (2018) demonstram que fraudes e burlas acarrectam prejuízos bilionários, afectando tanto empresas privadas quanto instituições públicas (p. 141). Além das perdas directas, há também custos indirectos, como investimentos adicionais em segurança, auditorias e sistemas de *compliance*.

Isso gera um efeito cascata, encarecendo produtos e serviços para consumidores e enfraquecendo a competitividade nacional e internacional.

Do ponto de vista psicológico, Santos (2020) destaca que vítimas de burla frequentemente experimentam sentimentos de vergonha, impotência e ansiedade, podendo desenvolver até quadros depressivos (p. 203). Para o autor, a burla não causa apenas um dano patrimonial, mas um trauma emocional que pode levar a desconfiança crônica em relações futuras. Esse impacto subjectivo mostra que a burla atinge dimensões profundas da vida humana, indo além da esfera material.

1.3 Burla no ambiente digital

1.3.1 Principais tipos de burlas *online* (*phishing*, falsos empregos, esquemas de investimento, vendas fraudulentas)

Segundo Ferreira (2016), o *phishing* é "a modalidade mais difundida de burla digital, baseada no envio de mensagens falsas que induzem o utilizador a fornecer credenciais pessoais ou bancárias" (p. 74). O autor sublinha que este tipo de fraude evoluiu com o tempo, passando de simples *emails* mal redigidos para páginas falsas altamente sofisticadas que simulam portais de bancos ou instituições públicas. A sua disseminação deve-se sobretudo à baixa literacia digital de muitos utilizadores.

De acordo com Mendes (2019), os falsos anúncios de emprego também representam uma modalidade crescente, explorando o desemprego estrutural e as aspirações da juventude (p. 118). Muitas vezes, os burladores exigem pagamentos antecipados para supostas formações, documentação ou taxas administrativas inexistentes. Esse esquema tem forte impacto em países africanos, onde o desemprego juvenil constitui um problema crítico.

Já Rodrigues & Costa (2021) destacam os esquemas de investimento e as vendas fraudulentas como fenómenos em expansão, sobretudo através de redes sociais e plataformas de comércio electrónico (p. 93). Nestes casos, os burladores prometem retornos financeiros irrealistas ou vendem produtos inexistentes, aproveitando a ausência de regulamentação eficaz do comércio digital. Para os autores, a combinação entre facilidade de acesso e fraca fiscalização torna este tipo de burla especialmente rentável para os criminosos.

1.3.2 Mecanismos utilizados pelos burladores (engenharia social, manipulação psicológica, tecnologias digitais)

Conforme Almeida (2015), a engenharia social é o principal mecanismo de exploração nas burlas digitais, uma vez que "em vez de atacar sistemas, o burlador manipula pessoas, explorando fragilidades emocionais e cognitivas" (p. 65). Isso pode incluir a criação de falsas narrativas de urgência, pedidos de ajuda ou promessas de recompensas. O alvo, assim, é induzido a agir contra os seus próprios interesses sem perceber o engano.

Para Sousa (2018), a manipulação psicológica é reforçada pelo uso de técnicas de persuasão que exploram factores como confiança, medo e autoridade (p. 102). Por exemplo, muitos golpes utilizam a identidade falsa de uma instituição bancária ou governamental para legitimar a abordagem. Esse mecanismo demonstra que a burla digital não depende apenas de tecnologia, mas de um profundo conhecimento do comportamento humano.

No campo tecnológico, Martins & Ribeiro (2020) observam que os burladores recorrem a *softwares* de *spoofing,* clonagem de *sites* e até inteligência artificial para automatizar ataques (p. 144). Segundo os autores, a sofisticação tecnológica permite aumentar a escala das fraudes, atingindo milhares de vítimas em simultâneo. O cruzamento entre manipulação psicológica e ferramentas digitais torna a burla mais difícil de identificar e combater.

1.3.3 Desafios do combate à burla digital em Angola

Segundo Chaves (2017), um dos maiores desafios no combate à burla digital em Angola reside na ausência de legislação específica e actualizada para lidar com crimes informáticos complexos (p. 89). Muitas vezes, os casos são enquadrados em normas genéricas de fraude ou abuso de confiança, o que dificulta a sua persecução penal. Esta lacuna jurídica abre espaço para a impunidade e fragiliza a confiança dos cidadãos nas instituições de justiça.

Já de acordo com António (2019), a escassez de recursos técnicos e humanos especializados constitui outro obstáculo significativo (p. 54). A investigação digital exige peritos em informática forense, capacidade de rastreamento de IPs e cooperação internacional, elementos ainda limitados em Angola. Tal fragilidade torna o país mais vulnerável a burlas transnacionais e dificulta a responsabilização dos autores.

Por fim, Lourenço & Pires (2021) destacam que a baixa literacia digital da população aumenta a eficácia das burlas e limita a prevenção (p. 127).

Muitos cidadãos não reconhecem sinais básicos de fraude *online*, como endereços electrónicos suspeitos ou promessas de ganhos fáceis. Os autores defendem que campanhas de sensibilização pública e educação digital são essenciais para reduzir a incidência desse fenómeno.

1.4 Cidadania e segurança digital

1.4.1 Literacia digital como ferramenta de prevenção da burla

Segundo Cardoso (2016), a literacia digital "não se limita ao domínio técnico de ferramentas, mas implica a capacidade crítica de avaliar informações e identificar potenciais riscos" (p. 72). Neste sentido, promover competências digitais entre cidadãos é fundamental para reduzir a vulnerabilidade diante de burlas *online*. A formação adequada permite reconhecer padrões de fraude e evitar comportamentos de risco no ciber-espaço.

Para Gomes & Oliveira (2019), em sociedades com baixa literacia digital a probabilidade de ocorrência de burlas *online* é significativamente mais elevada, pois os utilizadores tendem a confiar em qualquer informação recebida (p. 115). Os autores defendem que programas educativos em escolas e comunidades podem funcionar como barreira preventiva, fornecendo instrumentos de autoprotecção. Assim, a educação digital deve ser encarada como política pública estratégica.

Conforme Lopes (2021), a literacia digital deve ser entendida como um direito e um dever cívico, pois a protecção contra burlas *online* não é apenas responsabilidade das autoridades, mas também do cidadão informado (p. 38). Para o autor, investir na capacitação da população fortalece a segurança colectiva, tornando a sociedade menos vulnerável a redes fraudulentas. A prevenção, portanto, inicia-se pela formação crítica e consciente dos indivíduos.

1.4.2 Direitos e deveres dos cidadãos na protecção contra fraudes

Segundo Silva (2015), o cidadão digital tem o direito de usufruir de um ambiente *online* seguro, mas também o dever de adoptar comportamentos responsáveis, como proteger dados pessoais e utilizar canais oficiais de comunicação (p. 94). Esse equilíbrio entre direitos e deveres é essencial para que a sociedade digital funciona de forma confiável. Sem a colaboração individual, as políticas públicas tornam-se insuficientes.

De acordo com Martins (2018), os deveres dos cidadãos incluem a actualização regular de *softwares*, a utilização de senhas fortes e a não partilha de informações sensíveis em plataformas não seguras (p. 61).

Tais práticas reduzem o espaço de actuação dos burladores e fortalecem a resiliência colectiva contra-ataques digitais. O autor defende que a cidadania digital deve ser compreendida como prática diária de prevenção.

Já Rocha & Mendes (2020) sublinham que os direitos digitais também abrangem o acesso à informação transparente sobre riscos de fraude e aos mecanismos de protecção oferecidos pelas instituições (p. 140). Para eles, cabe ao Estado assegurar políticas de cibersegurança, mas aos cidadãos cabe utilizá-las com responsabilidade.

1.4.3 A importância da denúncia como instrumento de justiça e cidadania

Conforme Faria (2014), a denúncia de burlas desempenha um papel duplo: contribui para a responsabilização criminal dos autores e fortalece a confiança social no sistema de justiça (p. 83). O silêncio, por outro lado, perpetua a impunidade e favorece a expansão das práticas fraudulentas. A denúncia, portanto, constitui um acto de cidadania activa.

Segundo Pinto & Carvalho (2017), em muitos países africanos a subnotificação de fraudes está associada ao medo de represálias, à falta de confiança nas autoridades ou à vergonha das vítimas (p. 108). Isso enfraquece o combate institucional e limita a recolha de dados estatísticos fiáveis. Para os autores, criar canais acessíveis e confidenciais de denúncia é fundamental para inverter esse quadro.

Já Andrade (2021) argumenta que a denúncia deve ser entendida não apenas como mecanismo de justiça, mas como exercício de cidadania que contribui para o bem colectivo (p. 52). Ao denunciar, o indivíduo não protege apenas a si mesmo, mas também potenciais futuras vítimas. Assim, a cultura de denúncia fortalece a segurança digital e o sentido de responsabilidade social.

1.5 Legislação e normas sobre crimes digitais

1.5.1 Enquadramento legal internacional (ONU, União Africana, GDPR)

De acordo com Castells (2012), a ONU tem reiterado, em várias resoluções, a necessidade de cooperação internacional no combate ao cibercrime, visto que “os delitos digitais não conhecem fronteiras, tornando impossível um tratamento exclusivamente nacional” (p. 119). O autor lembra que documentos como a Convenção de Budapeste (2001) são referências mundiais, mesmo para países que não a retificaram, ao estabelecer normas mínimas para harmonização legislativa e cooperação judicial.

Segundo Okeke (2017), no contexto africano a União Africana aprovou a Convenção de Malabo sobre Cibersegurança e Protecção de Dados Pessoais (2014), que se apresenta como marco continental (p. 87).

A convenção propõe a criação de estruturas nacionais de cibersegurança e mecanismos de protecção de dados pessoais, estabelecendo um enquadramento legal adaptado à realidade africana. No entanto, a sua implementação tem sido lenta, devido às disparidades institucionais entre os Estados membros.

No plano europeu, Almeida & Rocha (2019) salientam que o Regulamento Geral de Protecção de Dados (GDPR) da União Europeia se tornou uma referência global, inclusive para países africanos que procuram alinhar-se a padrões internacionais (p. 141). Os autores destacam que, embora o GDPR não trata especificamente da burla, sua ênfase na protecção de dados pessoais fortalece a prevenção contra práticas fraudulentas. Assim, o enquadramento internacional actua como guia de boas práticas.

1.5.2 Leis angolanas relacionadas a crimes de burla e cibercrime

Conforme Quintino (2018), o Código Penal Angolano de 2020 incorporou disposições específicas sobre crimes informáticos, tipificando condutas como acesso ilegítimo a sistemas, falsificação informática e burla praticada por meios digitais (p. 62). Essa actualização representou um avanço em relação ao código anterior, alinhando o país às exigências da economia digital.

Segundo Chindombe (2021), a Lei n.º 7/17 sobre Protecção de Sistemas e Redes Informáticas constitui outro marco jurídico, ao estabelecer medidas de segurança obrigatórias para entidades públicas e privadas (p. 95). O autor sublinha que, embora ainda pouco conhecida pelo público, a lei é fundamental para responsabilizar empresas na adopção de mecanismos de prevenção contra burlas digitais.

Para Rocha (2022), a legislação angolana também contempla crimes de burla e abuso de confiança no Código Penal, reforçando que as modalidades digitais não se encontram fora do alcance do direito penal tradicional (p. 107). Contudo, o autor observa que muitas vezes os dispositivos legais são aplicados de forma fragmentada, gerando dúvidas sobre a sua eficácia prática.

1.5.3 Limitações e desafios na aplicação da legislação em Angola

De acordo com Pereira (2019), um dos principais desafios da aplicação das leis sobre cibercrime em Angola é a falta de formação técnica de magistrados e investigadores para lidar com evidências digitais (p. 55). Muitas vezes, provas electrónicas não são aceites em tribunal por falhas na sua recolha ou preservação. Isso fragiliza o combate ao crime digital, mesmo quando a lei prevê a punição.

Para Fonseca (2020), a ausência de uma cooperação internacional consolidada também limita a eficácia da legislação angolana (p. 133). Crimes digitais frequentemente envolvem servidores ou autores localizados fora do país, exigindo mecanismos de extradição e partilha de provas que ainda são frágeis. Essa limitação permite que muitos crimes permaneçam impunes.

Finalmente, Lopes & Mendes (2021) destacam que a aplicação da lei enfrenta obstáculos sociais, como a baixa taxa de denúncia e o desconhecimento da população sobre os mecanismos legais de protecção (p. 76). Para os autores, a eficácia das normas não depende apenas da sua existência formal, mas da conjugação de factores institucionais, técnicos e culturais.

1.6 Tecnologias *web* e plataformas de denúncia

1.6.1 Importância de *websites* como ferramentas de participação social

Segundo Castells (2009), a *internet* "transformou-se em espaço privilegiado de exercício da cidadania, ao permitir que indivíduos comunicam, participam e denunciam irregularidades sem barreiras físicas" (p. 117). Nesse contexto, *websites* tornam-se instrumentos essenciais para ampliar a voz dos cidadãos e reduzir o silêncio em torno de práticas fraudulentas.

De acordo com Mendes (2018), plataformas digitais de denúncia promovem transparência e *accountability*, funcionando como mediadores entre a sociedade civil e as instituições públicas (p. 63). O autor sublinha que tais *websites* têm potencial para reduzir a impunidade, pois criam canais alternativos à burocracia tradicional, muitas vezes marcada por lentidão ou corrupção.

Para Ferreira & Pinto (2020), o impacto social de *websites* de denúncia depende do grau de confiança que transmitem à população (p. 88). Quanto mais claros e acessíveis forem os mecanismos de participação, maior será a adesão dos cidadãos. Isso significa que a importância dessas ferramentas vai além da tecnologia: envolve credibilidade institucional e cultural.

1.6.2 Usabilidade, acessibilidade e segurança em *websites* de denúncia

Segundo Nielsen (2012), a usabilidade é condição indispensável para o sucesso de qualquer plataforma digital, pois "a dificuldade de navegação reduz drasticamente a participação dos utilizadores" (p. 41). No caso de *websites* de denúncia, menus claros, formulários intuitivos e *feedback* imediato são factores que estimulam o engajamento.

Conforme Lima (2019), a acessibilidade digital deve garantir que pessoas com deficiência, baixa literacia ou acesso limitado à tecnologia também possam usar plataformas de denúncia (p. 74). Isso implica aplicar directrizes internacionais, como *Web Content Accessibility Guidelines* (WCAG), adaptadas ao contexto local. A inclusão digital é um requisito ético e jurídico.

Para Martins & Sousa (2021), a segurança é outro eixo central, pois a denúncia muitas vezes envolve informações sensíveis que, se mal protegidas, podem expor a vítima a retaliações (p. 109). Os autores defendem a adopção de protocolos de encriptação, autenticação multifactorial e políticas de anonimato, a fim de assegurar protecção ao denunciante e credibilidade à plataforma.

1.6.3 Experiências internacionais de plataformas digitais contra a fraude

Segundo *Transparency* International (2017), países como Índia e Filipinas criaram *websites* governamentais de denúncia de corrupção que aumentaram significativamente o número de casos reportados (p. 53). A experiência demonstra que a digitalização amplia a participação cívica, sobretudo em contextos com limitações geográficas ou sociais.

De acordo com Wright & De Hert (2018), na União Europeia diversas plataformas digitais permitem a denúncia anónima de fraudes financeiras, beneficiando da protecção legal ao *whistleblower* (p. 92). Essas iniciativas reforçam a confiança dos cidadãos em denunciar, sabendo que seus direitos estão salvaguardados.

Já Carvalho (2020) destaca a experiência brasileira com o portal "Fala.BR", que centraliza denúncias de fraudes, corrupção e irregularidades em serviços públicos (p. 136). Segundo o autor, a plataforma funciona como modelo para outros países lusófonos, por combinar acessibilidade, transparência e integração com órgãos de controlo.

1.7 Ferramentas utilizadas para a criação do *website* StopBurla

1.7.1 PHP

Figura 1.

Fonte: https://cdn-icons-png.flaticon.com/512/5968/5968268.png

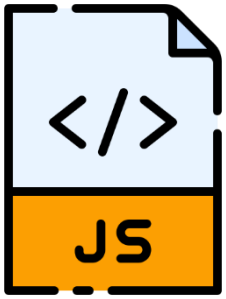
Segundo Ullman (2019), o PHP é "uma das linguagens de programação mais utilizadas para o desenvolvimento *web* dinâmico, permitindo a interacção entre a *interface* do utilizador e os bancos de dados" (p. 64). No presente projecto, o PHP foi empregado para implementar as funcionalidades principais do *website* StopBurla, como autenticação de utilizadores e processamento de formulários de denúncia.

De acordo com Welling & Thomson (2017), a flexibilidade do PHP permite integração simples com o *MySQL* e outras bases de dados relacionais, o que o torna ideal para aplicações que exigem manipulação constante de informações (p. 89). Essa característica foi determinante para a escolha da linguagem neste trabalho.

Para Souza (2020), a ampla comunidade de programadores PHP garante suporte técnico, documentação extensa e diversas bibliotecas de código aberto (p. 121). Assim, a utilização desta linguagem contribuiu para maior eficiência e redução do tempo de desenvolvimento.

1.7.2 *JavaScript*

Figura 2.



Fonte: https://cdn-icons-png.flaticon.com/512/10809/10809622.png

Segundo Flanagan (2018), o *JavaScript* "é a linguagem central da *web*, responsável por dotar as páginas de interactividade e dinamismo" (p. 52). No projecto, o *JavaScript* foi essencial para validar formulários de denúncia e fornecer respostas imediatas aos utilizadores.

De acordo com Resig & Bibeault (2016), *frameworks* e bibliotecas em *JavaScript*, como *jQuery*, ampliam a capacidade de criar *interfaces* ricas e responsivas, facilitando a experiência do utilizador (p. 73). Essas ferramentas foram exploradas para melhorar a usabilidade do *website* StopBurla.

Para Meyer (2021), o *JavaScript* desempenha papel crucial na implementação de boas práticas de segurança, como máscaras de entrada de dados e bloqueio de *scripts* maliciosos (p. 110). Neste sentido, sua aplicação contribuiu para aumentar a confiabilidade do sistema.

1.7.3 *Bootstrap*

Figura 3.

Fonte: https://flaticon.com/bootstrap

Conforme Spurlock (2015), o *Bootstrap* é um dos *frameworks* CSS mais populares, "permitindo o *design* de páginas responsivas que se adaptam automaticamente a diferentes dispositivos" (p. 44). O projecto utilizou essa ferramenta para garantir acessibilidade tanto em computadores como em dispositivos móveis.

Segundo MacDonald (2019), a padronização estética fornecida pelo *Bootstrap* reduz o tempo de desenvolvimento, assegurando ao mesmo tempo consistência visual entre páginas (p. 97). Essa característica foi essencial para manter o *website* StopBurla intuitivo.

Já Lima (2020) observa que o uso de componentes pré-desenvolvidos do *Bootstrap*, como botões e formulários, melhora significativamente a usabilidade, sem comprometer a identidade visual (p. 83). Essa vantagem foi aproveitada neste projecto para optimizar o tempo de implementação.

1.7.4 Cursor IA

Figura 4.

Fonte: https://custom.typingmind.com/assets/models/cursor.png

De acordo com Santos (2023), ferramentas de apoio baseadas em inteligência artificial, como o Cursor IA, "auxiliam programadores na geração de código, detecção de erros e optimização de algoritmos" (p. 59). No presente trabalho, o Cursor IA foi utilizado para acelerar o desenvolvimento e sugerir melhorias no código.

Segundo Costa & Ribeiro (2022), sistemas de apoio ao desenvolvimento baseados em IA reduzem a incidência de erros humanos, permitindo maior eficiência e precisão no processo de programação (p. 112).

Para Marques (2023), a integração de ferramentas de IA em ambientes de programação representa um avanço metodológico, pois amplia a capacidade criativa e técnica dos desenvolvedores (p. 138). Tal recurso contribuiu directamente para a qualidade do produto final.

1.7.5 *MySQL workbench*

Figura 5.

Fonte: https://flaticon.com/mysql

Segundo DuBois (2016), o *MySQL Workbench* é "a principal ferramenta de modelação, administração e *design* de bases de dados *MySQL*" (p. 102). Neste projecto, foi utilizada para estruturar as tabelas de utilizadores e denúncias.

De acordo com Stephens (2018), o *Workbench* permite uma visualização gráfica da arquitectura do banco de dados, facilitando a manutenção e a documentação do projecto (p. 67). Essa funcionalidade foi determinante para organizar as relações entre entidades.

Para Oliveira (2020), a integração com consultas SQL optimizadas torna o *MySQL Workbench* uma ferramenta essencial para projectos que exigem consistência e escalabilidade de dados (p. 93). Assim, o sistema de denúncias pode ser implementado de forma segura.

1.7.6 XAMPP

Figura 6.

Fonte: https://flaticon.com/xampp

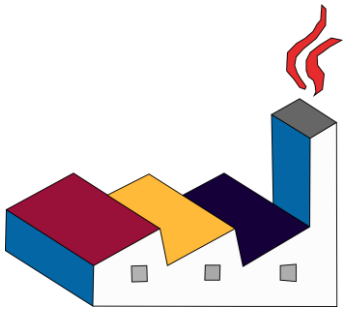
Segundo Welling & Thomson (2017), o XAMPP é "um pacote integrado que reúne Apache, *MySQL*, PHP e *Perl*, oferecendo um ambiente local completo para desenvolvimento *web*" (p. 142). Ele foi utilizado como servidor local para testar o *website* StopBurla.

Para Santos (2019), a simplicidade de instalação e configuração do XAMPP facilita o trabalho de programadores iniciantes e experientes (p. 88). Essa característica permitiu maior agilidade nas fases de testes.

Já Lima (2021) destaca que, além da facilidade, o XAMPP proporciona segurança ao simular fielmente o ambiente de produção, evitando falhas na migração (p. 59). Isso garantiu maior confiabilidade ao sistema desenvolvido.

1.7.7 *Plant*UML

Figura 7.



Fonte: https://flaticon.com/plantuml

Conforme Brown (2017), o *Plant*UML é "uma ferramenta que gera diagramas UML a partir de texto simples, permitindo rápida visualização de casos de uso e diagramas de classes" (p. 33). No presente projecto, foi usado para documentar visualmente a arquitectura do sistema.

Segundo Reis (2019), a utilização de UML em projectos de *software* é fundamental para alinhar os requisitos funcionais e não funcionais com a implementação prática (p. 71). O *Plant*UML facilitou essa integração ao permitir ajustes rápidos nos diagramas.

Para Moreira (2020), a clareza gráfica proporcionada por ferramentas como o *Plant*UML reduz ambiguidades entre desenvolvedores e garante melhor comunicação com *stakeholders* (p. 98). Desta forma, a modelação auxiliou tanto no desenvolvimento como na apresentação académica do trabalho.

CAPÍTULO II – APRESENTAÇÃO DO *WEBSITE STOPBURLA*

Neste capítulo, será apresentado o *website* StopBurla desenvolvido, descrevendo a sua estrutura, funcionalidades e principais componentes. Serão detalhados o processo de concepção, a arquitectura e a forma como cada módulo contribui para alcançar os objectivos propostos.

2.1 Metodologia utilizada para a criação do *website StopBurla*

Para a criação do *website* StopBurla foi utilizada a Metodologia de Desenvolvimento Iteractivo e Incremental (DII), combinada com princípios da investigação aplicada, de forma a unir a compreensão do fenómeno social da burla à implementação de uma solução tecnológica. Assim, adoptou-se uma abordagem mista que permitiu não apenas analisar o problema, mas também propor uma ferramenta prática de denúncia digital.

Neste projecto, a escolha pela metodologia incremental possibilitou a construção gradual do *website* StopBurla, com iteracções sucessivas, testes de usabilidade e segurança. Essa opção conferiu maior flexibilidade, permitindo incorporar ajustes à medida que novas necessidades foram identificadas durante o processo.

2.2 Requisitos funcionais (RF)

São as funcionalidades ou serviços que o sistema deve obrigatoriamente oferecer para atender às necessidades do usuário. Descrevem o que o sistema faz.

Tabela 1.

Requisitos Funcionais

Nº	Tipo	Requisito	Descrição
RF01	Funcional	Cadastro de usuário	O *Website* StopBurla permite que Usuários realizam cadastro mediante preenchimento de formulário com dados pessoais.

RF02	Funcional	Recuperação de senha	O *Website* StopBurla permite que Usuários recuperam a senha através de envio de *link* de redefinição por *email*.
RF03	Funcional	Edição de perfil	O *Website* StopBurla permite que Usuários editam seus perfis, actualizando seus dados.
RF04	Funcional	Exclusão de conta	O *Website* StopBurla permite que Usuários excluam sua conta.
RF05	Funcional	Registo de denúncia	O *Website* StopBurla permite que Usuários registam denúncias através de formulário com descrição e opcionalmente, envio de anexos.
RF06	Funcional	Consulta de denúncia	O *Website* StopBurla permite que Usuários consultam as denúncias registadas.
RF07	Funcional	Gestão de usuários	O *website* StopBurla permite que o Administrador faz gestão de contas de Usuários.

RF08	Funcional	Gestão de denúncias	O *website* StopBurla permite que o Administrador acompanha e analisa as denúncias registadas pelos Usuários.
RF09	Funcional	Painel estatístico	O *website* StopBurla permite que o Administrador acessa relatórios e estatísticas, incluindo número de usuários activos e denúncias registadas.

Fonte: Elaborado pelo autor, 2026.

2.3 Requisitos não funcionais (RNF)

São características de qualidade e restrições que o sistema deve atender, relacionadas como o sistema deve se comportar, mas não descrevem funcionalidades.

Tabela 2.

Requisitos não funcionais

Nº	Tipo	Requisito	Descrição
RNF01	Não funcional	Usabilidade	O *Website* StopBurla deve possuir *interface* intuitiva, com menus claros e consistentes, facilitando o uso.

RNF02	Não funcional	Desempenho	O tempo de resposta para carregamento de páginas e execução de operações não deve ultrapassar 3 segundos em condições normais de uso.
RNF03	Não funcional	Disponibilidade	O *Website* StopBurla deve estar disponível 24 horas por dia, 7 dias por semana, com tempo de indisponibilidade programada de no máximo 2% ao mês.
RNF04	Não funcional	Segurança	Todos os dados sensíveis (senhas, informações pessoais) devem ser armazenados de forma criptografada e transmitidos via HTTPS.
RNF05	Não funcional	Compatibilidade	A plataforma deve ser compatível com os principais navegadores modernos (*Chrome, Edge, Firefox*, Safari) e funcionar em dispositivos móveis e *desktop*.

RNF06	Não funcional	Escalabilidade	O *Website* StopBurla deve suportar crescimento no número de Usuários e Denúncias sem comprometer o desempenho.
RNF07	Não funcional	Confiabilidade	O *Website* StopBurla deve garantir integridade dos dados em caso de falhas, com *backups* automáticos diários.
RNF08	Não funcional	Manutenibilidade	O *Website* StopBurla deve ser desenvolvido com código modular e documentado, facilitando manutenção e futuras actualizações.
RNF09	Não funcional	Auditabilidade	Todas as acções críticas (cadastro, exclusão de conta, gestão de denúncia) devem ser registadas em *logs* acessíveis apenas pelo Administrador.

RNF10	Não funcional	Acessibilidade	O *Website* StopBurla deve seguir directrizes de acessibilidade (WCAG 2.1).

Fonte: Elaborado pelo autor, 2026.

2.4 Casos de uso

São descrições (geralmente em forma de cenários) que especificam como os usuários (actores) interagem com o sistema para alcançar um objectivo específico. Representam a execução prática de requisitos funcionais.

Tabela 3.

Casos de uso

Código	Nome do caso de uso	Actor(es)	Descrição
UC01	Efectuar cadastro	Usuário	O usuário preenche um formulário com dados pessoais para criar a conta.
UC02	Recuperar senha	Usuário, Administrador	O usuário solicita redefinição de senha e recebe um *link* de recuperação por *email*.
UC03	Editar perfil	Usuário, Administrador	O usuário actualiza seus dados pessoais no perfil.
UC04	Excluir conta	Usuário	O usuário excluir a sua conta.

UC05	Registar denúncia	Usuário	O usuário preenche um formulário para registar uma denúncia.
UC06	Consultar denúncias	Usuário	O usuário consulta as denúncias previamente registadas.
UC07	Gerir usuários	Administrador	O administrador faz a gestão das contas dos usuários.
UC08	Gerir denúncias	Administrador	O administrador acompanha, analisa e toma decisões sobre as denúncias registadas pelos usuários.
UC09	Visualizar painel estatístico	Administrador	O administrador acessa relatórios e estatísticas sobre usuários e denúncias.
UC10	Enviar notificações por e*mail*	*Website* (Automático)	O *Website* StopBurla envia *emails* automáticos para usuários após a recuperação da senha, cadastro e registo de denúncia.

Fonte: Elaborado pelo autor, 2026.

2.4.1 Descrição dos casos de uso

UC01 – Efectuar cadastro

- **Actor:** usuário
- **Objectivo:** permitir que o usuário cria uma conta no *website* StopBurla.
- **Descrição:** o usuário acessa a página de cadastro e preenche um formulário com informações pessoais (nome, *email*, senha, etc.). Após o envio, o sistema valida os dados e confirma a criação da conta.
- **Fluxo principal:**
    1. Usuário acessa a página de cadastro.
    2. Usuário preenche os dados obrigatórios.
    3. O *website* StopBurla valida os campos obrigatórios.
    4. Conta é criada e uma mensagem de sucesso é exibida.
    5. Usuário pode efectuar *login* com as credenciais criadas.

UC02 – Recuperar senha

- **Actor(es):** usuário, administrador
- **Objectivo:** possibilitar redefinição de senha em caso de esquecimento.
- **Descrição:** o actor solicita recuperação de senha informando o *email* cadastrado. O *website* StopBurla envia um *link* de redefinição por *email*. O actor acessa o *link* e cria uma nova senha.
- **Fluxo principal:**
    1. Actor acessa a página de recuperação de senha.
    2. Informa seu *email* cadastrado.
    3. O *website* StopBurla valida o *email* e gera *link* de redefinição.
    4. *Email* automático é enviado com instruções.
    5. Actor acessa o *link* e define uma nova senha.
- **Observações:** caso o *email* não esteja cadastrado, o sistema informa erro.

UC03 – Editar perfil

- **Actor(es):** usuário, administrador
- **Objectivo:** permitir actualização dos dados pessoais cadastrados.
- **Descrição:** o actor acessa seu perfil e altera informações como nome, *email* e senha. Após validação, os dados são actualizados no sistema.
- **Fluxo principal:**
    1. Actor faz *login*.
    2. Acessa área de perfil.
    3. Actualiza os campos desejados.
    4. O *website* StopBurla valida e grava as alterações.
    5. Mensagem de confirmação é exibida.

UC04 – Excluir conta

- **Actor:** usuário
- **Objectivo:** permitir que o usuário exclua sua conta.
- **Descrição:** o usuário decide encerrar sua conta no *website* StopBurla. Após autenticação, confirma a exclusão. O sistema remove os dados pessoais e torna a conta inacessível.
- **Fluxo principal:**
    1. Usuário faz *login*.
    2. Acessa configurações da conta.
    3. Solicita exclusão da conta.
    4. O *website* StopBurla solicita confirmação da acção.
    5. Conta é removida e mensagem final é exibida.
- **Observações:** a exclusão é irreversível.

UC05 – Registar denúncia

- **Actor:** usuário
- **Objectivo:** registar uma denúncia formal através do sistema.
- **Descrição:** o usuário acessa o formulário de denúncias, descreve o caso e, se necessário, anexa documentos em PDF. O sistema armazena a denúncia para posterior análise pelo administrador.
- **Fluxo principal:**
    1. Usuário faz *login*.
    2. Acessa o formulário de denúncia.
    3. Preenche os dados solicitados.
    4. (Opcional) Anexa documentos em PDF.
    5. O *website* StopBurla armazena a denúncia e envia confirmação.

UC06 – Consultar denúncias

- **Actor:** usuário
- **Objectivo:** permitir que o usuário acompanha suas denúncias registadas.
- **Descrição:** o usuário pode visualizar a lista de denúncias submetidas e verificar o estado de análise.
- **Fluxo principal:**
    1. Usuário faz *login*.
    2. Acessa área de denúncias registadas.
    3. O *website* StopBurla exibe lista com detalhes e estado.
- **Observações:** o usuário só visualiza suas próprias denúncias.

UC07 – Gerir usuários

- **Actor:** administrador
- **Objectivo:** permitir administração de contas de usuários.

- **Descrição:** o administrador pode visualizar contas de usuários.
- **Fluxo principal:**
    1. Administrador acessa painel de gestão de usuários.
    2. Visualiza lista de contas registadas.
- **Observações:** apenas o administrador possui este privilégio.

UC08 – Gerir denúncias

- **Actor:** administrador
- **Objectivo:** permitir que o administrador acompanha e analisa denúncias registadas.
- **Descrição:** o administrador pode visualizar as denúncias submetidas.
- **Fluxo principal:**
    1. Administrador acessa painel de denúncias.
    2. Visualiza lista de denúncias registadas.
    3. Analisa cada denúncia individualmente.

UC09 – Visualizar painel estatístico

- **Actor:** administrador
- **Objectivo:** obter visão geral das actividades do sistema.
- **Descrição:** o administrador acessa relatórios e estatísticas sobre quantidade de usuários e denúncias registadas.
- **Fluxo principal:**
    1. Administrador acessa área de estatísticas.
    2. O *website* StopBurla apresenta gráficos e relatórios detalhados.
- **Observações:** informações são apenas de leitura.

UC10 – Enviar notificações por *email*

- **Actor:** *website* (automático)
- **Objectivo:** informar usuários sobre eventos importantes via *email*.

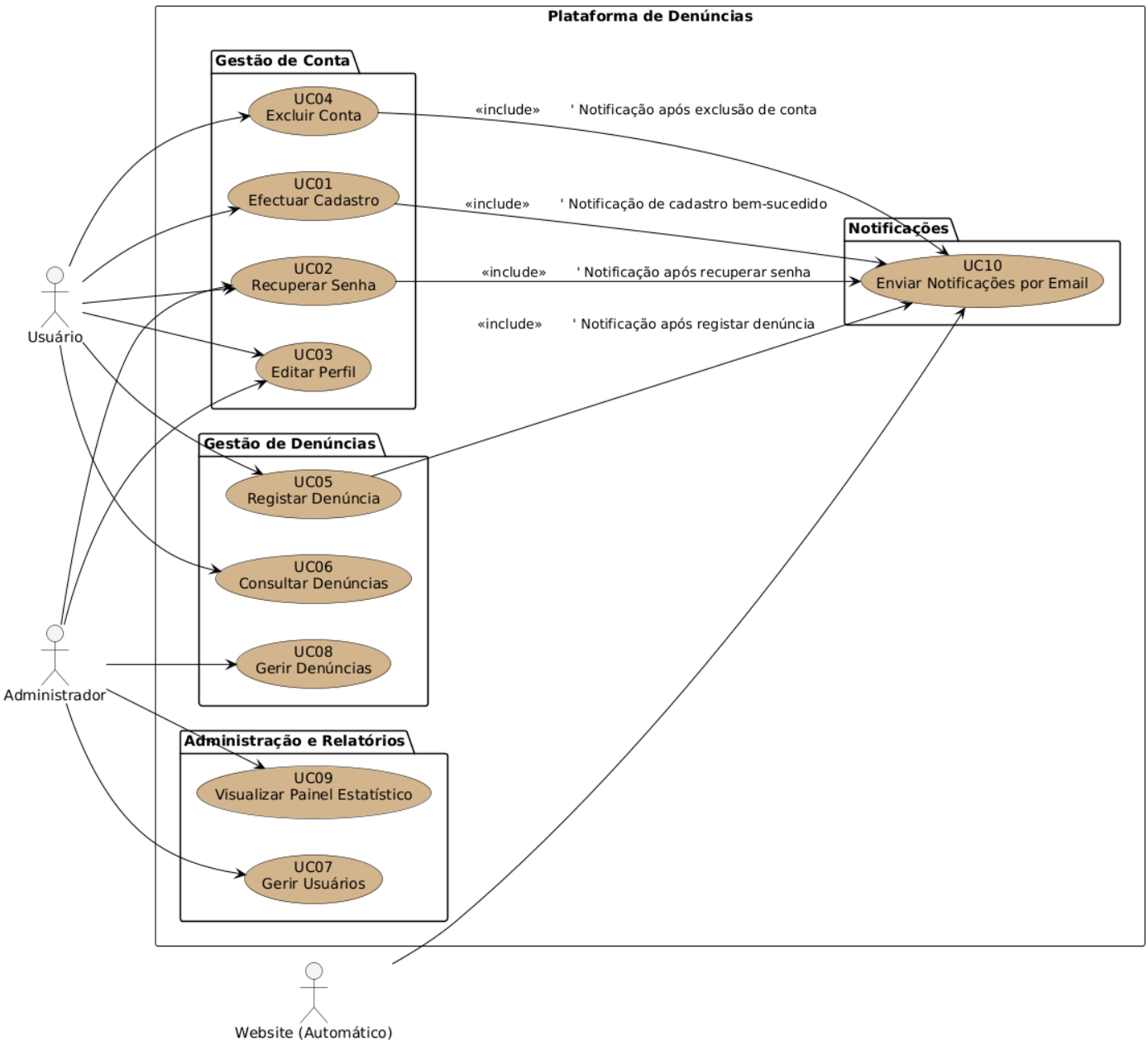
- **Descrição:** o sistema envia notificações automáticas quando há recuperação de senha ou registo de denúncia.
- **Fluxo principal:**
    1. Acção do usuário (recuperar senha ou registar denúncia) é concluída.
    2. O *website* StopBurla gera *email* automático.
    3. *Email* é enviado ao destinatário.
- **Observações:** o envio é automático, sem intervenção humana.

2.5 Diagrama de caso de uso

É um diagrama da UML que descreve as funcionalidades (casos de uso) que o sistema deve oferecer e como os actores (usuários ou sistemas externos) interagem com ele.

Figura 8.

Diagrama de caso de uso



Fonte: Elaborado pelo autor, 2026.

Figura 8 – Diagrama de caso de uso: este diagrama representa, de forma gráfica, as principais funcionalidades disponíveis para os actores do sistema, destacando o papel do Usuário, do Administrador e do *Website* Automático. O usuário pode efectuar cadastro, recuperar senha, editar o perfil, excluir a conta, registar e consultar denúncias, enquanto o administrador é responsável por gerir usuários, gerir denúncias e visualizar estatísticas no painel.

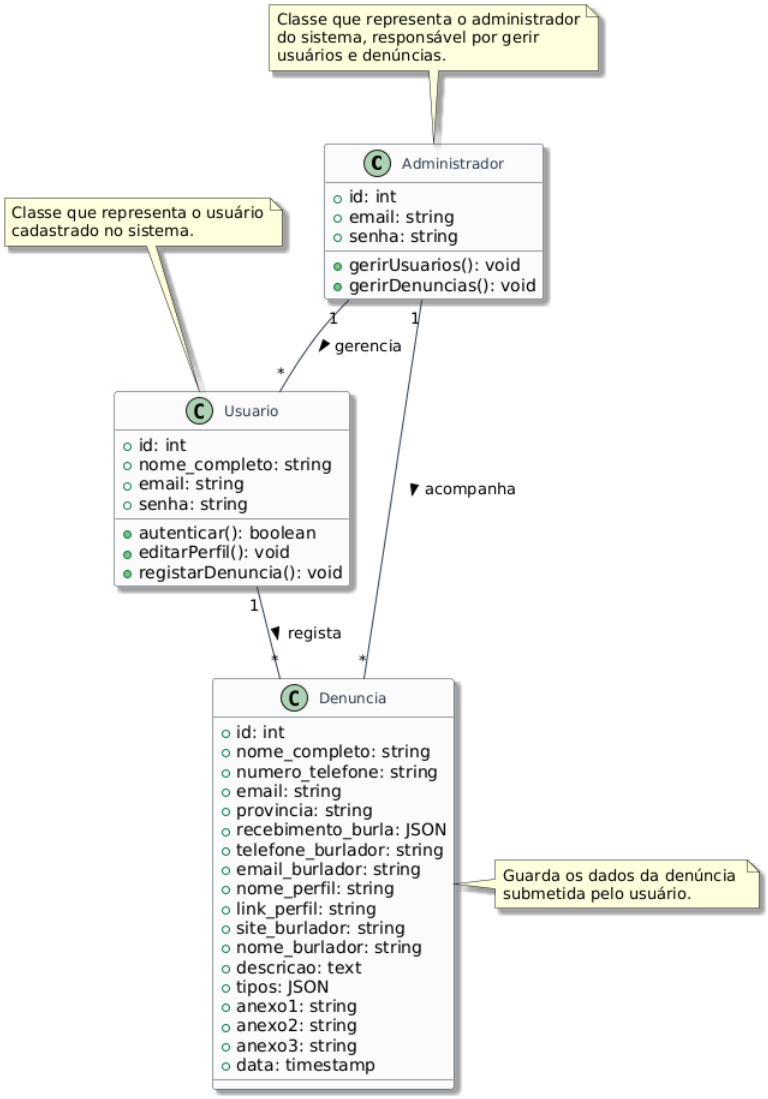
Já o *website* StopBurla, de forma automática, envia notificações por *email* para confirmar operações importantes como cadastro, recuperação de senha, exclusão de conta e registo de denúncia. Este diagrama mostra a interacção entre actores e funcionalidades, bem como as relações de inclusão entre casos de uso dependentes.

2.6 Diagrama de classe

É um diagrama da UML que representa a estrutura estática do sistema, mostrando classes, atributos, métodos e os relacionamentos entre elas (associação, herança, composição etc.).

Figura 9.

Diagrama de classe



Fonte: Elaborado pelo autor, 2026.

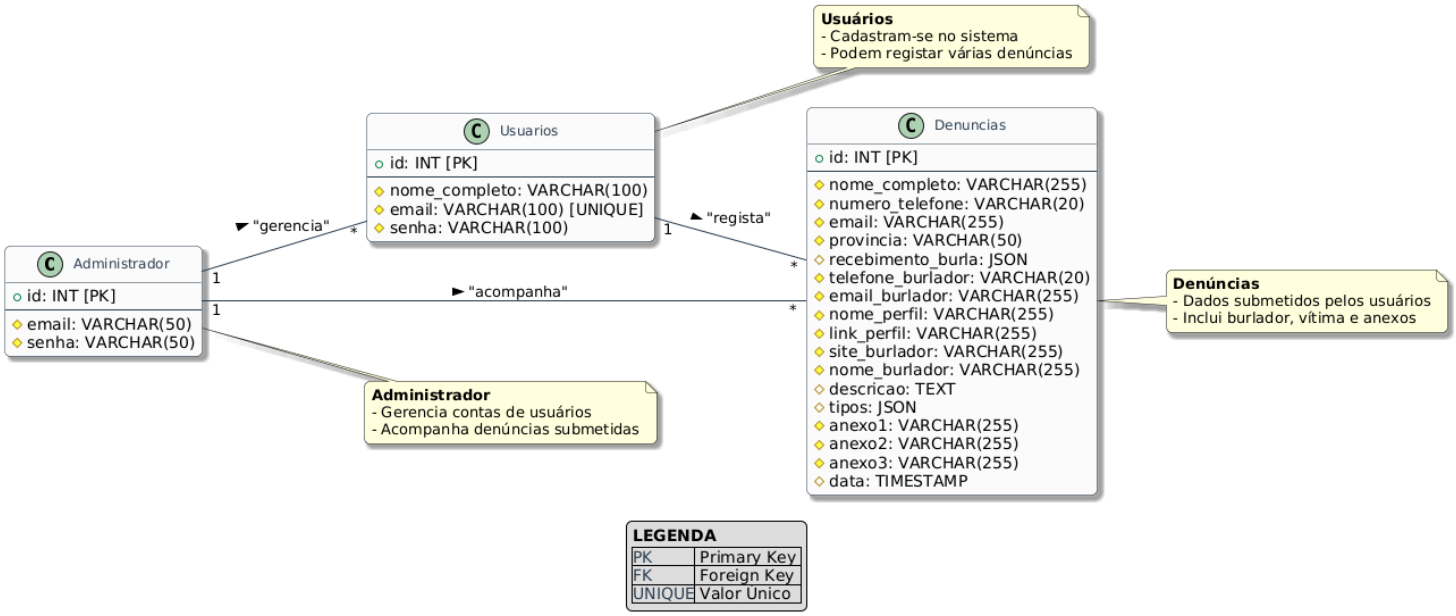
Figura 9 – Digrama de classe: este diagrama representa as estruturas de dados e operações do sistema stop_burla, mostrando as classes principais Administrador, Usuario e Denuncia com os seus atributos (por exemplo id, *email*, senha em Administrador e Usuario; em Denuncia atributos detalhados como nome_completo, numero_telefone, recebimento_burla em JSON, descricao, anexo1/2/3, data, etc.) e métodos ricos (ex.: autenticar(), editarPerfil(), registarDenuncia(), gerirUsuarios()). As relações indicam que um Usuário pode registar múltiplas Denúncias (1 → *), enquanto o Administrador tem relações de supervisão/gestão tanto com usuários como com denúncias (1 → *), fornecendo uma visão orientada a objectos de como instâncias e comportamentos se organizam na aplicação.

2.7 Diagrama entidade-relacionamento (ER)

É um modelo usado em banco de dados que representa entidades (tabelas), atributos (colunas) e relacionamentos entre elas.

Figura 10.

Diagrama entidade-relacionamento (ER)



Fonte: Elaborado pelo autor, 2026.

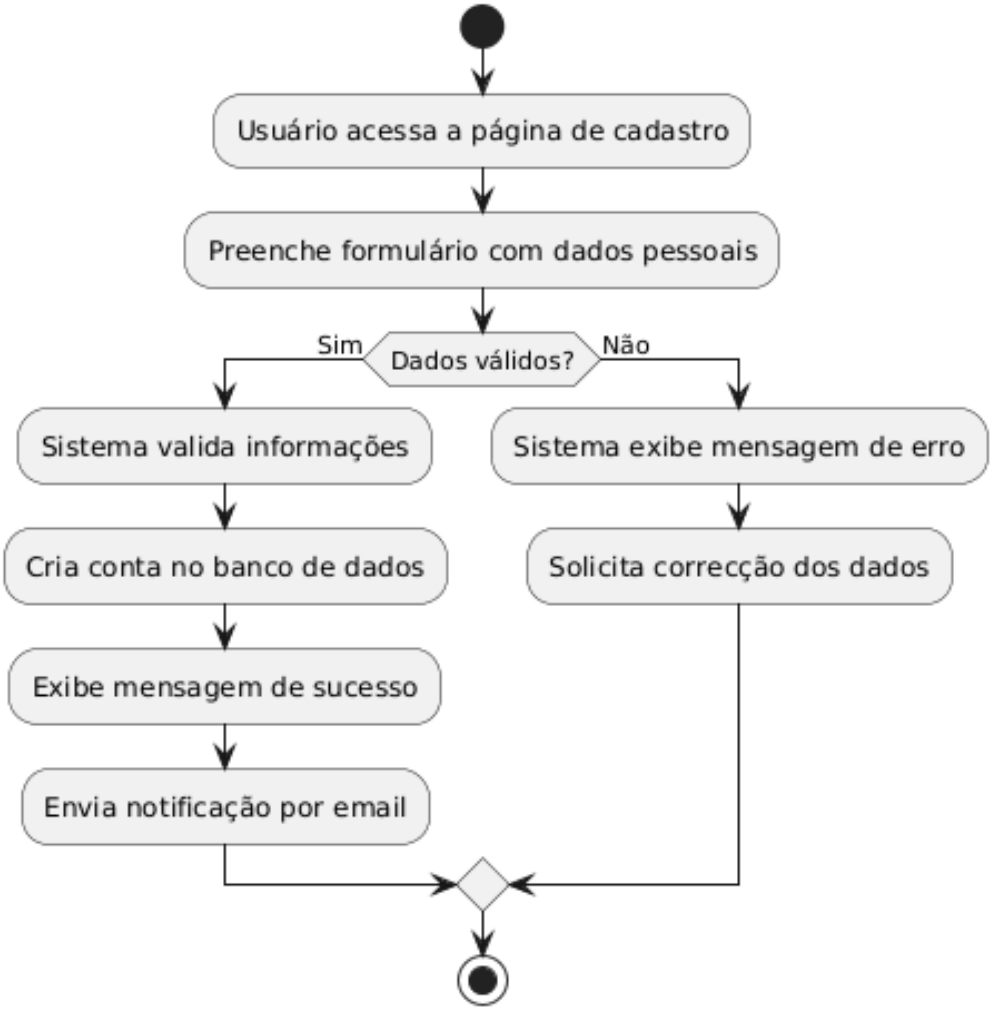
Figura 10 – Diagrama entidade-relacionamento: este diagrama traduz o esquema relacional da base de dados stop_burla em entidades e restrições: entidades Administrador, Usuarios e Denuncias com as suas chaves primárias (id) e atributos (incluindo colunas com restrições UNIQUE como *email* em usuarios, e campos JSON e TIMESTAMP em denuncias), além da legenda para PK/UNIQUE/FK.

2.8 Diagrama de actividade

É um diagrama da UML usado para modelar fluxos de trabalho ou processos, representando a sequência de actividades, decisões e paralelismos.

Figura 11.

Diagrama de actividade (Efectuar cadastro)



Fonte: Elaborado pelo autor, 2026.

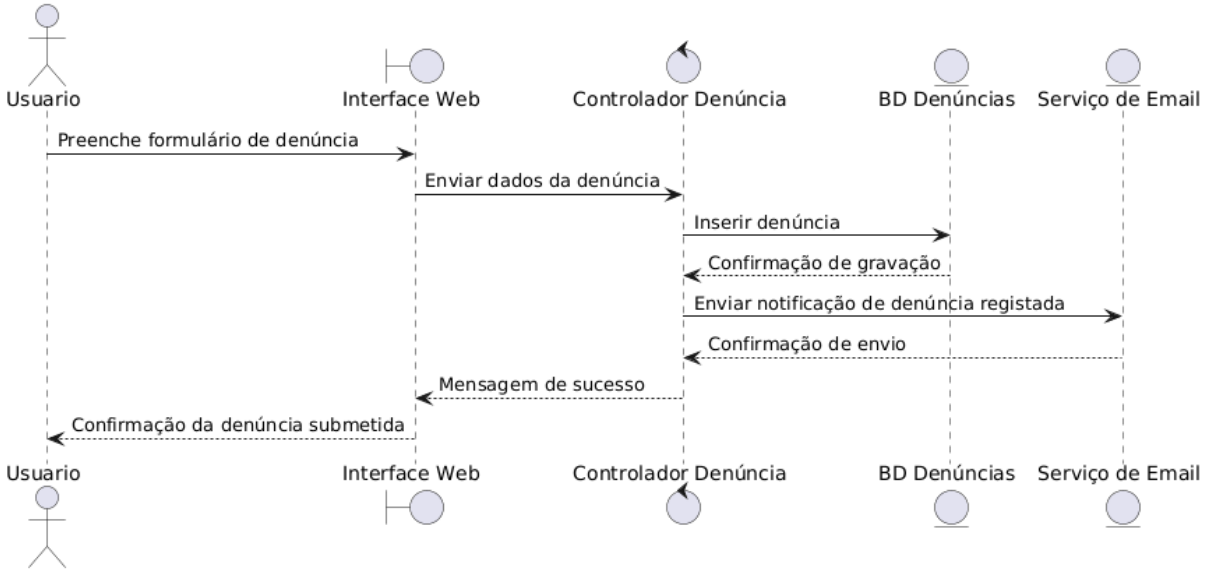
Figura 11 – Diagrama de actividade: este diagrama descreve o fluxo de acções realizadas quando um usuário efectua o cadastro no sistema. O processo inicia com o acesso à página de cadastro e o preenchimento do formulário com dados pessoais. Em seguida, o sistema valida os dados fornecidos, verificando se são válidos. Caso sejam aceitos, o sistema cria a conta no banco de dados, exibe uma mensagem de sucesso e envia uma notificação por *email* ao usuário. Se os dados forem inválidos, o sistema apresenta uma mensagem de erro e solicita que o usuário corrija as informações, repetindo o processo até que o cadastro seja concluído com sucesso.

2.9 Diagrama de sequência

É um diagrama da UML que descreve a interacção entre objectos ao longo do tempo, destacando a ordem cronológica das mensagens trocadas.

Figura 12.

Diagrama de sequência (Registar denúncia)



Fonte: Elaborado pelo autor, 2026.

Figura 12 – Diagrama de sequência: este diagrama representa o fluxo de submissão de uma denúncia num sistema *web*, iniciando-se com o Usuário, que preenche o formulário de denúncia através da *Interface Web*; em seguida, os dados são enviados ao Controlador de Denúncia, responsável por processar a informação e registá-la na Base de Dados de Denúncias, que devolve uma confirmação de gravação; após o registo bem-sucedido, o controlador aciona o Serviço de *Email* para o envio de uma notificação confirmando que a denúncia foi registada, recebendo igualmente a confirmação do envio.

CONCLUSÃO

A análise da problemática evidenciou que a carência de plataformas específicas de denúncia representa uma das maiores limitações no combate à burla, contribuindo para a subnotificação dos casos e para a perpetuação do fenómeno. A proposta de criação do *website* StopBurla buscou responder essa lacuna, estruturando-se com base em princípios de usabilidade, acessibilidade e segurança, de modo a atender às necessidades tanto das vítimas quanto das instituições responsáveis pela investigação e prevenção.

Conclui-se, portanto, que a pesquisa trouxe contribuições relevantes tanto para a academia quanto para a sociedade, ao propor uma solução tecnológica inovadora e adequada ao contexto angolano. Ainda que reconheça limitações relacionadas à abrangência do estudo e à necessidade de maior envolvimento institucional, o trabalho abre caminhos para futuros aperfeiçoamentos, como a integração com órgãos de justiça, o desenvolvimento de aplicativos móveis e a ampliação das funcionalidades de monitorização. Desta forma, reafirma-se a pertinência do tema e o potencial do *website* StopBurla como ferramenta essencial no combate à burla em Angola.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, J. (2016). *Burla, confiança social e coesão comunitária*. Lisboa: Lidel.

Almeida, R. (2015). *Engenharia social e crimes informáticos*. Lisboa: FCA.

Almeida, R., & Rocha, P. J. (2019). *Protecção de dados pessoais e regulação digital*. Coimbra: Almedina.

Andrade, P. S. (2021). Denúncia e cidadania digital: Uma abordagem sociojurídica. *Revista Africana de Direito e Sociedade, 6*(1), 45–60.

António, M. L. (2019). *Cibercrime e investigação criminal em Angola*. Luanda: Mayamba Editora.

Brandt, R. (2007). *Fraud and deception in medieval and modern law*. Berlin: Springer.

Cardoso, F. J. (2016). *Literacia digital e cidadania na sociedade da informação*. Porto: Vida Económica.

Carvalho, E. M. (2020). Plataformas digitais de denúncia e controlo social no Brasil. *Revista Brasileira de Administração Pública, 54*(2), 121–142.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age*. Cambridge: Polity Press.

Chaves, D. M. (2017). Desafios jurídicos do combate ao crime informático em Angola. *Revista Angolana de Ciências Jurídicas, 3*(2), 75–96.

Chindombe, A. L. (2021). *Cibersegurança e protecção de sistemas informáticos em Angola*. Luanda: Mayamba Editora.

Costa, P., & Ramos, L. (2020). *Criminalidade digital e burla electrónica*. Coimbra: Almedina.

Faria, L. R. (2014). *Cidadania, justiça e participação social*. Coimbra: Almedina.

Ferreira, J. A. (2016). *Segurança da informação e burla digital*. Lisboa: Lidel.

Ferreira, J. A., & Pinto, R. S. (2020). Websites de denúncia e confiança institucional. *Revista Lusófona de Comunicação e Sociedade, 7*(1), 75–94.

Fonseca, H. M. (2020). Cooperação internacional e repressão ao cibercrime em África. *Revista Africana de Relações Internacionais, 11*(2), 121–139.

Fragoso, H. C. (2012). *Lições de direito penal: Parte especial* (Vol. 2). Rio de Janeiro: Forense.

Gomes, A. R., & Oliveira, M. T. (2019). Educação digital e prevenção de fraudes online. *Revista Lusófona de Educação e Tecnologia, 5*(2), 101–120.

Gomes, M. A. (2017). *Cibercrime e segurança da informação*. São Paulo: Saraiva.

Kimani, J., & Wanjiku, M. (2017). Digital fraud and mobile money scams in Africa. *African Journal of Information Systems, 9*(3), 201–223.

Lima, S. R. (2019). *Acessibilidade digital e inclusão social*. Lisboa: FCA.

Lopes, C. M. (2021). *Cidadania digital e direitos fundamentais*. Coimbra: Almedina.

Lopes, C. M., & Mendes, J. F. (2021). Desafios socioculturais na aplicação da legislação sobre cibercrime. *Revista Angolana de Estudos Jurídicos, 5*(2), 65–82.

Lourenço, H. F., & Pires, J. S. (2021). Literacia digital e vulnerabilidade às burlas online em África. *Revista Africana de Tecnologia e Sociedade, 8*(1), 115–134.

Martins, J. P. (2018). *Cidadania digital e segurança da informação*. Lisboa: FCA.

Martins, R. A., & Ribeiro, T. S. (2020). Tecnologias emergentes e burla digital. *Revista Portuguesa de Cibersegurança, 4*(2), 133–152.

Martins, R. A., & Sousa, L. T. (2021). Segurança da informação em plataformas de denúncia digital. *Revista Portuguesa de Sistemas de Informação, 9*(2), 97–115.

Mbiti, J. S. (2007). *African religions and philosophy*. Oxford: Heinemann.

Mendes, L. F. (2018). Plataformas digitais, transparência e participação cidadã. *Revista Africana de Governação Electrónica, 4*(1), 55–70.

Mendes, L. F. (2019). Fraudes online e falsas oportunidades de emprego. *Revista de Estudos Sociais Africanos, 7*(2), 109–125.

Nielsen, J. (2012). *Usability engineering*. San Francisco, CA: Morgan Kaufmann.

Nnoli, O. (2003). *Introduction to politics*. Enugu: Snaap Press.

Okeke, C. N. (2017). Cybersecurity and data protection in Africa: The Malabo Convention. *African Journal of International Law, 5*(1), 73–94.

Oliveira, R. M. (2019). *Burla, fraude e cibercrime: Distinções essenciais no direito penal contemporâneo*. Coimbra: Almedina.

Pereira, J. M. (2019). Prova digital e processo penal em Angola. *Revista Angolana de Ciências Criminais, 3*(1), 43–60.

Pinto, A. M. (2008). *Criminalidade económica e sociedade da informação*. Lisboa: AAFDL.

Pinto, A. M., & Carvalho, S. F. (2017). Denúncia, confiança institucional e combate à fraude em África. *Revista Africana de Políticas Públicas, 9*(1), 97–114.

Pinto, A. M., & Carvalho, S. F. (2018). Impactos económicos da fraude no sector público e privado. *Revista de Economia e Gestão, 18*(2), 123–149.

PricewaterhouseCoopers. (2018). *Angola: Economic crime and fraud survey*. Luanda: PwC.

Quintino, J. M. (2018). *A fraude fiscal e os crimes afins em Angola*. Luanda: Mayamba Editora.

Rocha, E. L., & Mendes, C. J. (2020). Direitos digitais e políticas de cibersegurança. *Revista de Direito e Tecnologia, 6*(2), 129–148.

Rocha, P. J. (2022). Crimes de burla e cibercrime no direito penal angolano. *Revista de Direito Penal Africano, 6*(1), 95–113.

Rodrigues, V. P., & Costa, N. M. (2021). Investimentos online e novas formas de burla digital. *Revista Ibero-Americana de Economia Digital, 10*(1), 85–102.

Santos, L. F. (2020). Impactos psicológicos da vitimização por burla. *Revista Lusófona de Psicologia, 12*(1), 189–210.

Schulz, F. (2007). *Classical Roman law*. Oxford: Oxford University Press.

Silva, J. P. (2015). *Cidadania digital e protecção do consumidor online*. Porto: Vida Económica.

Silva, J. P. (2015). *Criminalidade patrimonial e desenvolvimento social*. Porto: Vida Económica.

Silva, J. P., Mendes, R., & Andrade, C. (2020). Prevenção da fraude no sistema bancário angolano. *Revista Angolana de Auditoria e Compliance, 4*(1), 45–63.

Sousa, M. R. (2018). *Psicologia da persuasão e burla digital*. Coimbra: Almedina.

Tavares, J. M. (2011). *Direito penal económico*. Coimbra: Coimbra Editora.

Transparency International. (2017). *People and corruption: Asia Pacific – Global corruption barometer*. Berlin: Transparency International.

Wright, D., & De Hert, P. (2018). *Enforcing privacy: Regulatory, legal and technological approaches*. Cham: Springer.

https://cdn-icons-png.flaticon.com/512/5968/5968268.png

https://cdn-icons-png.flaticon.com/512/10809/10809622.png

https://flaticon.com/bootstrap

https://custom.typingmind.com/assets/models/cursor.png

https://flaticon.com/mysql

https://flaticon.com/xampp

https://flaticon.com/plantuml

APÊNDICES

Apêndice n.º 1 – Guia de observação.

Este guião de observação integra-se na análise do fenómeno das burlas em Angola, tendo como principal objectivo recolher dados empíricos que permitem compreender o comportamento social dos cidadãos e as formas mais comuns de burla. Através da observação directa, foi possível acompanhar de perto situações e atitudes que evidenciam as fragilidades na comunicação e na sensibilização pública sobre medidas de prevenção. A observação incidiu sobre os aspectos relacionados às práticas fraudulentas, meios utilizados e reacções dos indivíduos, fornecendo subsídios essenciais para o delineamento das funcionalidades do *website* StopBurla.

Título da pesquisa:

Criação de um *Website* para Denúncia de Burla em Angola.

Tipo de observação:

Observação directa.

Objectivo geral:

Criar um *Website* para Denúncia de Burla.

1. Identificação

Tabela 4.

Identificação da observação

Elemento	Descrição
Local da observação	Diversos espaços públicos e digitais (ruas, mercados, redes sociais, instituições públicas e privadas).
Período de observação	Julho a Setembro de 2025
Observador	Ivânio Quiosa
População observada	Cidadãos angolanos de diferentes faixas etárias e ocupações.

Fonte: Elaborado pelo autor, 2026.

2. Aspectos a observar

Tabela 5.

Aspectos a observar

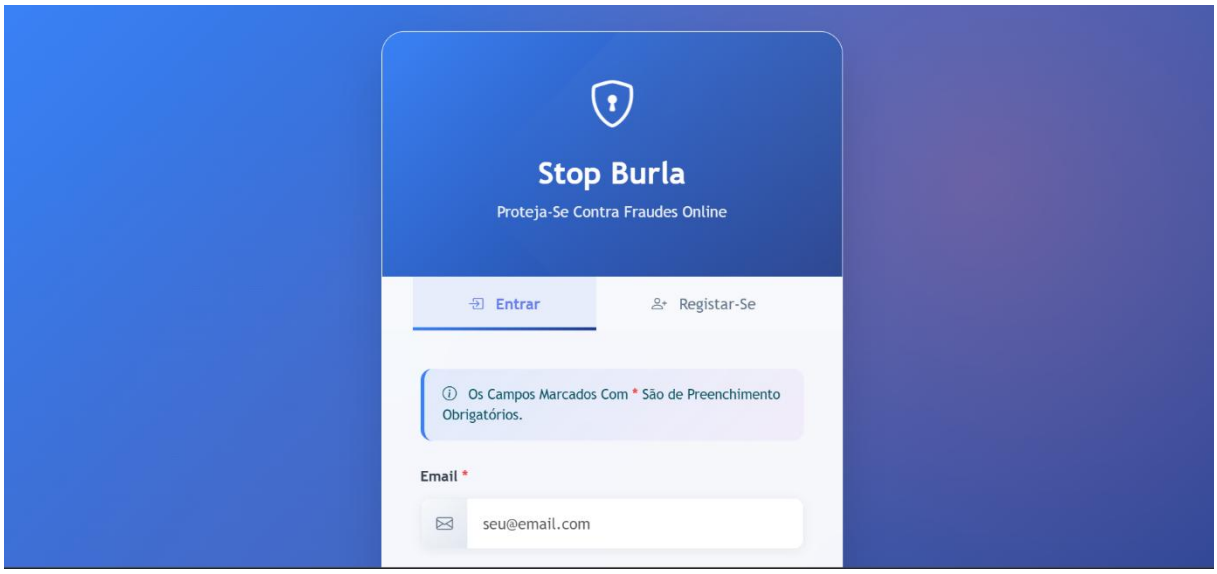
Categoria	Elementos de observação	Indicadores / Perguntas de apoio
A. Formas de burla	Tipos mais comuns de burla identificados.	Que tipo de burla é mais recorrente (presencial, telefónica, *online*, bancária, etc.)?
B. Meios utilizados pelos burladores	Recursos e estratégias de engano.	Quais são os principais meios usados (telefone, redes sociais, *email*, pessoalmente)?
C. Reacção dos cidadãos	Comportamento face a possíveis burlas.	Como os cidadãos reagem quando percebem ou são alvos de burla?
D. Nível de conhecimento preventivo	Grau de informação sobre medidas de prevenção.	Os cidadãos sabem identificar uma burla? Conhecem formas de evitar?
E. Comunicação e sensibilização Pública	Existência e eficácia de campanhas preventivas.	Existem acções públicas de sensibilização? São eficazes?
F. Impacto social	Consequências económicas e emocionais.	Como a burla afecta as vítimas e a sociedade em geral?

Fonte: Elaborado pelo autor, 2026.

Apêndice n.º 2 – Algumas telas do *website* StopBurla.

Figura 13.

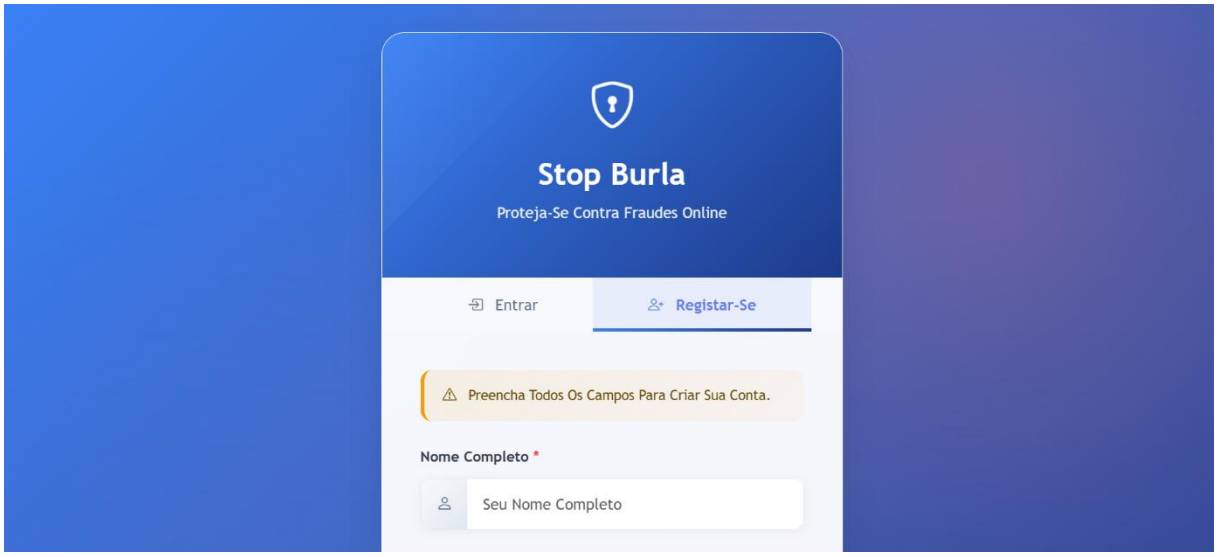
Tela de login



Fonte: Elaborado pelo autor, 2026.

Figura 14.

Tela de cadastro



Fonte: Elaborado pelo autor, 2026.

Figura 15.

Painel do website StopBurla

Fonte: Elaborado pelo autor, 2026.

Figura 16.

Formulário de denúncias

Fonte: Elaborado pelo autor, 2026.

Figura 17.

Painel do administrador

Fonte: Elaborado pelo autor, 2026.