INSTITUTO SUPERIOR POLITÉCNICO DE CIÊNCIAS E TECNOLOGIA

CURSO DE CIÊNCIAS CRIMINAIS

Desenvolvimento de uma Plataforma Digital com Base a Ánalise do Inquérito de Vitimização Criminal e Percepção de Segurança no Município da Samba, no ano 2025

Autoras:Celina Elizabeth José

Clementina Katchinombelo Ulombe

Orientador: Juan Rúbem Herrera Masó

Luanda-2025

INSTITUTO SUPERIOR POLITÉCNICO DE CIÊNCIAS E TECNOLOGIA

CURSO DE CIÊNCIAS CRIMINAIS

Desenvolvimento de uma Plataforma Digital com Base a Ánalise do Inquérito de Vitimização Criminal e Percepção de Segurança no Município da Samba, no ano 2025

Autoras:Celina Elizabeth José

Clementina Katchinombelo Ulombe

Orientador: PhD. Juan Rúbem Herrera Masó

Luanda-2025

INSUTEC
INSTITUTO SUPERIOR POLITÉCNICO
DE CIÊNCIAS E TECNOLOGIA

DECLARAÇÃO DE APROVAÇÃO DO ORIENTADOR

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

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

Luanda, aos_____de_____de 20_____

_____

Assinatura do Orientador

Luanda-2025

TERMO DE APROVAÇÃO

Nós, Celina Elizabeth José e Clementina Katchinombelo Ulombe, certificamos que este trabalho é original _____,_____.

Tema: Desenvolvimento de uma Plataforma Digital para Monitoramento da Vitimização Criminal e Percepção de Segurança no Município da Samba, no ano 2025

"Trabalho de Conclusão de Curso apresentado ao Instituto Superior Politécnico de Ciências e Tecnologia como parte dos requisitos para obtenção de grau académico de Licenciatura em Ciências Criminais"

Esta monografia foi avaliada e aprovada para a obtenção do título de licenciada no curso Ciências Criminais.

_____

Orientador

_____

Presidente do Júri

_____

Arguente

_____

Arguente

AGRADECIMENTOS

Primeiramente, agradecemos a Deus pela força, sabedoria e perseverança que nos permitiram concluir esta etapa tão importante de nossas vidas académicas.

Expressamos nossa sincera gratidão aos nossos familiares, pelo apoio incondicional, incentivo constante e compreensão nos momentos de dedicação intensa ao trabalho. Sem vocês, esta jornada teria sido muito mais difícil.

Agradecemos também aos nossos professores e, em especial, ao nosso orientador PhD. Juan Rúbem Herrera Masó e ao Msc Rouget Ruano, pela paciência, orientação, ensinamentos e pela confiança depositada em nosso potencial, contribuindo de forma essencial para a concretização deste trabalho.

Aos colegas Alice Matumba, Eliane Manuel, Edivaldo Augusto, Jussara Andrade, Luyana De Castro e Mause Lima, agradecemos pela colaboração, incentivo e companheirismo ao longo desta caminhada académica, tornando os desafios mais leves e as conquistas mais significativas.

De forma especial eu Clementina, expresso a minha profunda gratidão à Unitel, pelo apoio concedido através da bolsa de estudos, que possibilitou a minha formação académica e contribuiu significativamente para a realização deste sonho.

Por fim, agradecemos a todos que, de alguma forma, contribuíram para a realização deste trabalho, direta ou indiretamente, tornando possível a sua conclusão.

RESUMO

A vitimização criminal constitui um fenómeno complexo que impacta directamente a segurança pública, a formulação de políticas de prevenção e a percepção de segurança das populações. Em contextos urbanos, a ausência de sistemas centralizados para a recolha, organização e análise de dados de vitimização criminal contribui para a fragmentação da informação, dificultando o acompanhamento das vítimas e a identificação de padrões criminais. Neste sentido, o presente trabalho tem como objectivo geral desenvolver uma plataforma digital com base na análise de inquéritos de vitimização criminal e percepção de segurança no município da Samba, no ano de 2025, com vista a contribuir para a melhoria da recolha e gestão de dados e apoiar as políticas de segurança pública e de prevenção criminal. A pesquisa adopta uma abordagem mista, combinando métodos quantitativos e qualitativos, com recurso à pesquisa bibliográfica e à pesquisa de campo, através da aplicação de inquéritos à população local. Os resultados esperados apontam para uma melhoria na sistematização dos dados, maior acessibilidade à informação e apoio à tomada de decisão por parte das instituições responsáveis pela segurança pública. Conclui-se que a integração entre Ciências Criminais e Engenharia Informática, por meio de plataformas digitais, pode fortalecer estratégias de prevenção criminal e promover políticas públicas mais eficazes e baseadas em evidências.

Palavras-chave: Plataformas digitais; Inquérito de vitimização criminal; Percepção de segurança.

ÍNDICE

LISTA DE TABELAS

INTRODUÇÃO

A vitimização criminal constitui, a nível mundial, um fenómeno complexo que ultrapassa a mera ocorrência do crime, envolvendo dimensões sociais, psicológicas, económicas e institucionais. A literatura internacional tem demonstrado que os dados provenientes dos registros oficiais não conseguem captar, de forma integral, a real magnitude da criminalidade, uma vez que uma parcela significativa das vítimas opta por não denunciar os crimes sofridos. Esta limitação compromete a capacidade dos Estados em compreender o fenómeno criminal e em formular políticas públicas eficazes e orientadas para a prevenção.

Neste sentido, os inquéritos de vitimização criminal assumem um papel central ao possibilitarem a recolha directa de informações junto das vítimas, permitindo identificar padrões de vitimização, factores de risco e níveis de percepção de segurança. A produção desse tipo de informação contribui para uma visão mais abrangente da criminalidade, ao integrar dados quantitativos e qualitativos que não se encontram disponíveis nos sistemas tradicionais de registo. A eficácia desses inquéritos depende, em grande medida, da forma como os dados são recolhidos, organizados, armazenados e analisados.

Com o avanço das tecnologias digitais, observa-se uma crescente aposta no uso de plataformas digitais como instrumentos de apoio à recolha e gestão de dados no domínio da segurança pública. Essas plataformas possibilitam a sistematização das informações, a redução da fragmentação dos dados e a melhoria do acesso por parte de investigadores, gestores públicos e instituições responsáveis pela segurança. Assim, a articulação entre inquéritos de vitimização criminal, percepção de segurança e plataformas digitais revela-se fundamental para o fortalecimento da gestão da informação e para a tomada de decisões baseadas em evidências.

No contexto angolano, a criminalidade urbana representa um desafio relevante para a segurança pública, particularmente nas grandes cidades, onde factores como crescimento populacional acelerado, desigualdades sociais e fragilidades institucionais contribuem para a complexidade do fenómeno criminal. Apesar dos esforços das autoridades, persistem dificuldades na recolha e gestão sistemática de dados sobre vitimização criminal, o que limita a capacidade de avaliação das políticas de prevenção e controlo do crime.

A dependência predominante dos registos oficiais tende a invisibilizar experiências de vitimização não denunciadas, bem como as percepções de insegurança vivenciadas pela população. Esta lacuna informacional compromete a formulação de estratégias preventivas eficazes, uma vez que as decisões são tomadas com base em dados incompletos ou pouco organizados. Torna-se, portanto, necessário investir em mecanismos que permitam organizar e sistematizar os dados de vitimização criminal de forma estruturada e acessível.

Neste cenário, o uso de plataformas digitais surge como uma alternativa capaz de melhorar a recolha, a gestão e a análise dos dados relacionados à vitimização criminal e à percepção de segurança. Ao permitir o acesso integrado à informação, essas

plataformas podem apoiar as instituições responsáveis pela segurança pública, promovendo maior eficiência na análise dos dados e contribuindo para decisões mais informadas no planeamento de políticas públicas de segurança e prevenção criminal.

A nível local, a província de Luanda apresenta características específicas que intensificam os desafios relacionados à vitimização criminal, destacando-se a elevada densidade populacional e a diversidade de contextos socioeconómicos. O município da Samba insere-se nesse contexto urbano complexo, onde as dinâmicas sociais e espaciais influenciam tanto a ocorrência dos crimes quanto a percepção de segurança da população residente.

A inexistência de sistemas ou plataformas digitais centralizadas para a recolha e análise de inquéritos de vitimização no município dificulta a identificação de padrões criminais e a localização de áreas mais vulneráveis. A dispersão dos dados impede uma leitura integrada do fenómeno, limitando o acompanhamento das vítimas e reduzindo a eficácia das estratégias de prevenção criminal adoptadas a nível comunitário.

Diante desse contexto, torna-se pertinente o desenvolvimento de uma plataforma digital orientada para a análise de inquéritos de vitimização criminal e percepção de segurança no município da Samba. Ao possibilitar a organização estruturada dos dados, a plataforma poderá apoiar a identificação de áreas de risco, facilitar o acesso à informação por parte das autoridades e contribuir para uma compreensão mais aprofundada da vitimização criminal. Assim, o estudo propõe-se a reforçar a tomada de decisão no planeamento de políticas de segurança pública, integrando os contributos das Ciências Criminais e da Engenharia Informática.

Problematização

A vitimização criminal constitui um desafio significativo para a segurança pública e para a formulação de politicas públicas em Angola, sobretudo na província de Luanda, que concentra uma elevada taxa de densidade populacional (equivalente á 5.349,3 habitantes segundo o último relatório síntese dos dados definitivos do CENSO em 2024) e uma diversidade de contextos socieconómicos.

A ausência de sistemas ou plataformas centralizados há registros e análises de inquéritos de vitimização criminal contribui para a fragmentação das informações, dificultando o acompanhamento necessário ás vítimas, a identificação de padrões criminais e a avaliação de políticas de prevenção. Além disso, a dispersão dos dados podem de certa forma comprometer a confiabilidade de estudos sobre vitimização criminal, tornando difícil mensurar com precisão o impacto social e económico do crime na capital angolana. Diante deste contexto, surge a necessidade de desenvolver uma plataforma digital com base a ánalise de inquéritos de vitimização criminal e percepção de segurança, capaz de consolidar os dados de forma segura, confiável e acessível, promovendo uma base empírica robusta para pesquisadores, gestores públicos, profissionais das áreas de segurança pública e a sociedade em geral.

Problema de pesquisa

Como o desenvolvimento de uma plataforma digital com base a ánalise do inquérito de vitimização criminal e percepção de segurança, no município da Samba ,no ano 2025 contribuiu na recolha e a gestão de dados para melhorar as políticas de segurança pública e de prevenção de crimes?

Hipótese

O desenvolvimento de uma plataforma digital baseada em inquéritos de vitimização criminal e percepção de segurança melhora a gestão, organização e análise dos dados, permitindo a identificação de áreas de risco no município da Samba, contribuindo para a prevenção criminal e para a tomada de decisões mais informadas no planeamento de políticas de segurança pública.

Objectivo geral:

- Desenvolver uma plataforma digital com base na análise do inquérito de vitimização criminal e percepção de segurança no município da Samba, integrando os fundamentos das Ciências Criminais e da Engenharia Informática, com o propósito de contribuir para a melhoria da gestão de dados e para o fortalecimento das políticas de segurança pública e de prevenção de crimes.

Objectivos específicos:

- Fundamentar, à luz da literatura científica, os conceitos de vitimização criminal, percepção de segurança, inquéritos de vitimização, plataformas digitais e metodologias ágeis de desenvolvimento de software, estabelecendo o quadro teórico interdisciplinar que sustenta a investigação;
- Analisar a vitimização criminal e a percepção de segurança no município da Samba, através da aplicação de inquéritos à população residente, produzindo os dados de domínio que fundamentam e alimentam a plataforma digital;
- Construir a plataforma digital utilizando a metodologia Extreme Programming (XP) e tecnologias modernas de desenvolvimento web (React, Next.js, Node.js, Prisma ORM, SQLite), integrando funcionalidades de recolha, gestão, análise estatística e consulta inteligente dos dados;
- Validar a plataforma com os dados reais de vitimização criminal recolhidos no município da Samba, verificando a sua adequação funcional e a sua utilidade para o apoio à tomada de decisão em segurança pública.

Justificativa

A criminalidade traz consigo impactos significativos para aqueles que são vítimas, sejam eles económicos, sociais e psicológicos. Do ponto de vista social, ela pode gerar medo e insegurança de frequentar lugares públicos e andar durante um determinado período. Não obstante aos registros oficiais de crimes, indícios apontam para a não denúncia de crimes por parte de algumas vítimas, em alguns casos por medo de represálias ou dificuldades de acesso aos meios de denúncia.

É importante ter-se atenção para aqueles que sofrem directa ou indirectamente os impactos negativos do crime, pois, sem considerar a vítima somente analisamos estatísticas e números mas não o sofrimento humano. As políticas que não centralizarem a sua atenção as experiências de vitimização podem certamente falhar em diminuir o medo ou a sensação de insegurança mesmo que combata a criminalidade. Ao estudar sobre a vitimzação criminal é possível identifcar grupos mais vulneráveis e desenvolver estratégias preventivas direcionadas.

A análise não deve se limitar ao registro do crime em si mas também á experiência de vitimização criminal e a percepção de segurança da comunidade. Isso permitirá que os dados recolhidos sirvam para auxiliar na criação de estratégias de prevenção mais humanas e eficientes tendo em consideração tanto a acção do criminoso quanto os efeitos sobre as vítimas.

Portanto, este estudo se justifica por sua relevância social, académica e tecnológica, ao propor uma solução inovadora para enfrentar lacunas importantes na gestão e prevenção da criminalidade em Angola através do desenvolvimento de uma plataforma digital com base a análise de inquéritos de vitimização criminal e percepção de segurança, pois possibilita a recolha sistemática, organização e interpretação de dados, aprofundando tanto a ocorrência de crimes quanto aos seus efeitos sobre a população.

Novidade científica

A pesquisa pode dialogar com áreas como Sociologia, Psicologia, Criminologia, Engenharia Informática, ampliando a compreensão do tema e incentivando a colaboração entre disciplinas. Do ponto de vista científico, o estudo se justifica pela escassez de pesquisas e dados sistematizados sobre vitimização criminal em Angola. A produção de conhecimento estruturado sobre padrões de crime, perfis de vítimas e incidência de diferentes tipos de delitos contribui para preencher essa lacuna acadêmica e apoiar estudos futuros sobre segurança urbana e políticas de prevenção criminal em Angola.

Metodologia de pesquisa

Segundo a natureza, trata-se de uma pesquisa aplicada uma vez que busca desenvolver uma solução prática que responda a problemas específicos enfrentados pela vitimização criminal através da criação de uma plataforma digital capaz de armazenar dados com o propósito de auxiliar nas políticas de segurança pública, de prevenção e conecte quem esteja interessado em saber mais sobre o assunto. Também possui a componente básica

pois fundamenta-se teoricamente em estudos sobre vitimização criminal, percepção de segurança e plataformas digitais, ampliando o conhecimento científico sobre esses fenómenos.

Segundo os objectivos, trata-de de uma pesquisa descritiva e exploratória. É exploratória por permitir maior familiariadade com o problema e identificação de variáveis relevantes e descritiva por possibilitar a identificação dos tipos de crimes, e as percepções da população do município da Samba tem sobre a segurança. Esse tipo de pesquisa é apropriado quando se quer obter mais familiaridade com um problema pouco conhecido, identificar fatores relevantes e propor hipóteses para estudos futuros.

Segundo a abordagem, trata-se de uma pesquisa mista (quantitativa e qualitativa) porque busca compreender, por meio de análises interpretativas e subjetivas, as experiências, fornecendo uma visão mais abrangente e completa sobre o tema estudado. Integrando informações qualitativas, relativas à percepção de segurança e experiências de vitimização com dados quantitativos.

Segundo o procedimento, trata-se de uma pesquisa bibliográfica através da revisão de literatura sobre vitimização criminal, percepção de segurança e plataformas digitais, juntamente com a pesquisa de campo com a aplicação de inquéritos no município da Samba .

Métodos teóricos

Método de análise-síntese: a pesquisa adota o método analítico, utilizado para decompor e examinar criticamente os conceitos de vitimização criminal, percepção de segurança, plataformas digitais e políticas de segurança pública. O método sintético é empregado para integrar os conhecimentos provenientes das Ciências Criminais e da Engenharia Informática, possibilitando a construção de uma abordagem interdisciplinar.

Método indutivo-dedutivo: o método indutivo é utilizado na interpretação dos dados empíricos recolhidos por meio dos inquéritos de vitimização, permitindo a generalização de padrões observados no município da Samba. Juntamente com o método dedutivo que orienta a análise dos dados a partir das teorias da vitimização criminal e da percepção de segurança.

Hipotetico dedutivo- este método se baseia em uma estrutura lógica de formulação e verificação de hipóteses, permitindo uma análise rigorosa do tema. Facilita a validação científica do sistema proposto, verificando se a coleta, organização e análise de inquéritos realmente contribuem para uma melhor compreensão da vitimização criminal.

Suporta a construção de possíveis soluções baseadas em evidências, permitindo que conclusões gerais sobre padrões de crime e lacunas institucionais sejam derivadas a partir de dados concretos coletados no município da Samba .

Métodos empíricos

Método estatístico: consiste na utilização de técnicas matemáticas e ferramentas de análise de dados para coletar, organizar, analisar, interpretar e apresentar informações

quantitativas de forma sistemática e objetiva. Em pesquisas acadêmicas, ele permite transformar dados brutos em informações significativas, possibilitando identificar padrões, relações, tendências e variações dentro do objeto de estudo.

Técnicas de recolha de dados : diversidade de técnicas de recolha de dados permitirá um estudo abrangente e com maior rigor científico. Foram utlizadas duas técnicas principais:

- Inquérito por questionário: o questionário permite coletar dados padronizados e quantificados sobre as experiências das vítimas , frequência de crimes e factores associados a subnotificação, facilitando análises estatísticas e comparações em diferentes grupos.
- Observação directa: fornece informações qualitativas sobre registros e atendimento às vítimas, complementando os dados do questionário.

Caracterização da População e Amostra

Para a selecção da amostra utilizou-se uma amostragem probabilística estratificada. A população é dividida em estratos (grupos) e amostras são sorteadas de cada estrato proporcionalmente. , levando em consideração três critérios principais:

- Idade – para identificar percepções distintas entre jovens, adultos e idosos sobre segurança e vitimização.
- Género – para analisar possíveis diferenças na vitimização criminal e no medo do crime entre homens e mulheres.
- Localização dentro do município – para compreender se determinadas áreas do município são mais vulneráveis à criminalidade do que outras.

A amostra está formada por 522 indivíduos, com idades compreendida dos 18 á mais de 55 anos de idade.

Estrutura da monografia

A presente monografia apresenta a seguinte organização: elementos pré-textuais, elementos textuais e elementos pós-textuais.

Elementos pré-textuais: contêm informações essenciais que permitem ao leitor compreender de forma clara o contexto e o objeto de estudo da pesquisa.

Elementos textuais: correspondem à parte central do trabalho, na qual o tema é desenvolvido de maneira detalhada e estruturada em três segmentos principais:

Introdução: apresenta a contextualização do estudo, a delimitação do problema, os objetivos e o referencial teórico-metodológico adotado;

Capítulo I – Fundamentação teórica que dedica-se à exposição e análise dos conceitos, teorias e estudos realizados por outros autores que embasam a pesquisa;

Capítulo II – Análise de dados e desenvolvimento da plataforma digital.

O trabalho encerra-se com as conclusões, nas quais se destacam os principais achados e implicações do estudo, seguidas da lista de referências bibliográficas que subsidiaram a elaboração da pesquisa.

CAPÍTULO I: FUNDAMENTAÇÃO TEÓRICAS

1.1 Evolução histórica da vítima e dos inquéritos de vitimização criminal.

Durante grande parte da história do direito penal, a vítima ocupou uma posição secundária, sendo progressivamente afastada do centro do processo penal com a consolidação do Estado moderno e do monopólio estatal da punição (Fattah, 2010).

Segundo Fattah (2010), "com a ascensão do sistema moderno de justiça criminal, a vítima foi gradualmente afastada e marginalizada em favor do infractor e do Estado" (p. 23).

A vitimologia surge como campo científico autónomo a partir da década de 1940, com os trabalhos pioneiros de Hans von Hentig e Benjamin Mendelsohn, que passam a analisar a vítima como elemento central na compreensão do fenómeno criminal (Von Hentig, 1948; Mendelsohn, 1956).

Von Hentig (1948) afirmava que "a vítima desempenha um papel funcional no processo criminal e não pode ser excluída da análise criminológica" (p. 12).

Paralelamente ao desenvolvimento da vitimologia, emergiu a necessidade de instrumentos empíricos capazes de captar a criminalidade para além das estatísticas policiais, dando origem aos primeiros inquéritos de vitimização criminal nas décadas de 1960 e 1970 (Van Dijk, Van Kesteren & Smit, 2014).

Segundo Van Dijk et al. (2014), "os inquéritos de vitimização foram desenvolvidos para medir a criminalidade conforme experienciada pela população, independentemente dos dados oficiais da polícia." (p. 15).

A institucionalização destes inquéritos, sobretudo com o National Crime Victimization Survey (NCVS) e o International Crime Victims Survey (ICVS), consolidou a vítima como fonte legítima de dados científicos e como actor relevante na formulação de políticas públicas de segurança (Killias, van Kesteren & Mayhew, 2016).

1.2.1 Conceito de inquérito de vitimização criminal e a sua classificação

Etimologicamente, o termo inquérito deriva do latim inquirere, que significa investigar, examinar ou procurar informações de forma sistemática, enquanto vitimização provém do latim victima, designando aquele que sofre um dano ou prejuízo decorrente de uma acção criminosa (Cunha & Cintra, 2019).

No campo científico, o inquérito de vitimização criminal é definido pelo UNODC como "um inquérito estruturado que recolhe informações directamente junto dos indivíduos sobre as suas experiências de vitimização criminal, independentemente de os crimes terem sido denunciados ou não à polícia" (UNODC, 2010, p. 1).

Van Dijk (2015) acrescenta que estes inquéritos permitem medir tanto a incidência criminal como a percepção de segurança, ao afirmar que "os inquéritos de vitimização fornecem informações únicas sobre padrões de criminalidade e sentimentos de insegurança da população" (p. 69).

Quanto a classificação dos inquéritos de vitimização criminal, a literatura distingue essencialmente (Killias et al., 2016). :

a) Inquéritos nacionais de vitimização: os inquéritos nacionais são pesquisas de larga escala que cobrem todo o território de um país, permitindo gerar dados representativos da população sobre vitimização criminal.

Segundo Van Dijk (2015), estes inquéritos fornecem informações sobre a prevalência de crimes, padrões de vitimização e percepções de segurança, essenciais para orientar políticas públicas de segurança a nível nacional.

b) Inquéritos locais ou comunitários: os inquéritos locais ou comunitários são realizados em áreas geográficas específicas, como bairros, distritos ou cidades, com o objetivo de compreender a dinâmica da criminalidade a nível micro.

Van Dijk (2015) sublinha que estes inquéritos são particularmente úteis para detectar padrões de crime em comunidades específicas e avaliar a percepção de segurança em contextos locais.

c) Inquéritos sectoriais, dirigidos a grupos específicos: Os inquéritos sectoriais são focados em populações ou grupos específicos, como estudantes, trabalhadores, idosos ou profissionais de determinado setor, visando identificar tipos particulares de vitimização e riscos associados (Fattah, 2010).

Segundo Fattah (2010), esses inquéritos permitem analisar vulnerabilidades específicas e exposições a crimes particulares, fornecendo informações detalhadas que podem orientar medidas preventivas direcionadas e programas de proteção.

Killias et al. (2016) esclarecem que "os inquéritos de vitimização locais são particularmente úteis para compreender a dinâmica da criminalidade ao nível do bairro" (p. 41), o que os torna adequados para contextos urbanos angolanos.

Relativamente aos tipos de vitimização, a Vitimologia identifica a vitimização directa, quando o indivíduo sofre directamente o crime; a vitimização indirecta, quando familiares ou pessoas próximas são afectadas. Uma segunda tipologia apresenta-se em :

- Vitimização primária

A vitimização primária ocorre quando a vítima sofre diretamente o ato criminoso, sendo o alvo inicial do crime. Segundo Hindelang, Gottfredson e Garofalo (1978), este tipo de vitimização é o ponto de partida para a análise criminológica, pois permite identificar os fatores que tornam indivíduos ou grupos mais vulneráveis. Exemplos incluem furtos, assaltos, agressões físicas ou crimes sexuais, onde há contato direto entre o criminoso e a vítima.

- Vitimização secundária

A vitimização secundária acontece quando a vítima é re-traumatizada pelas respostas institucionais ou sociais inadequadas, como procedimentos policiais insensíveis, atrasos na justiça ou exposição pública de informações pessoais resultante do contacto inadequado com instituições formais (Fattah, 2010).

Segundo Fattah (2010), "a vitimização secundária ocorre quando as vítimas são re-traumatizadas pelas respostas institucionais" (p. 87).

Este tipo de vitimização destaca a importância de políticas públicas e sistemas de proteção que respeitem e preservem a dignidade da vítima, prevenindo danos adicionais. A literatura indica que plataformas digitais podem ajudar a reduzir a vitimização secundária ao organizar dados de forma segura e permitir respostas mais rápidas (Van Dijk, 2015).

- Vitimização terciária

A vitimização terciária refere-se ao impacto indireto ou simbólico do crime sobre familiares, amigos ou comunidades da vítima. Segundo Fattah (2010), este tipo de vitimização evidencia que a criminalidade não afeta apenas a vítima direta, mas também grupos sociais conectados, alterando percepções de segurança e confiança institucional.

No contexto angolano, compreender a vitimização terciária é fundamental para políticas de prevenção e programas de apoio comunitário, considerando o impacto coletivo de crimes como assaltos, violência urbana ou homicídios.

1.2.2 Teorias da Vitimização Criminal à luz do Contexto Angolano

A vitimização criminal constitui um fenómeno social que não se limita à ocorrência de crimes, mas envolve a experiência da vítima e os impactos sociais, psicológicos e económicos decorrentes do delito (Fattah, 2010). No contexto angolano, onde as estatísticas criminais oficiais podem não refletir totalmente a realidade urbana, a compreensão da vitimização depende tanto da análise de dados objetivos quanto da percepção subjetiva de segurança da população (Alemika, 2015).

As teorias da vitimização criminal oferecem modelos explicativos para entender quem é mais vulnerável, em que contextos ocorre a vitimização e quais fatores sociais, ambientais e individuais contribuem para ela, fornecendo uma base científica para políticas públicas de prevenção e intervenção.

a) Teoria do Estilo de Vida (Lifestyle Theory)

A Teoria do Estilo de Vida, desenvolvida por Hindelang, Gottfredson e Garofalo (1978), propõe que a probabilidade de uma pessoa ser vítima de crime está relacionada aos seus hábitos, rotinas diárias e padrões de interação social. Indivíduos que frequentam certos locais, horários ou ambientes de risco têm maior exposição à criminalidade.

No contexto angolano, esta teoria ajuda a compreender como comportamentos urbanos, deslocamentos diários e interações sociais influenciam a vulnerabilidade à vitimização.

Por exemplo, cidadãos que vivem ou circulam em bairros com pouca iluminação, alto índice de criminalidade ou falta de policiamento podem apresentar maior risco de vitimização (Alemika, 2015).

Esta teoria fundamenta a importância de recolher dados detalhados sobre hábitos e experiências da população, permitindo que políticas de segurança sejam direcionadas para reduzir a exposição ao risco e aumentar a sensação de proteção da comunidade.

b) Teoria da Vitimização Repetida (Repeat Victimization Theory)

A Teoria da Vitimização Repetida, proposta por Farrell e Pease (1993), sustenta que certos indivíduos, grupos ou locais têm maior probabilidade de serem vítimas de crimes de forma recorrente. Essa vulnerabilidade pode derivar de fatores individuais, sociais ou ambientais que tornam a vítima ou o local mais atraente ou mais exposto à ação criminosa.

No contexto angolano, a aplicação desta teoria é fundamental para identificar padrões de criminalidade e vulnerabilidade recorrente, permitindo que as autoridades planeiem ações preventivas mais precisas. Por exemplo, bairros com maior incidência de furtos ou assaltos podem ser monitorizados com base em dados de vitimização, evitando que padrões de crime se repitam e aumentando a eficácia das políticas de segurança (Van Dijk, 2015).

A integração dessa teoria com plataformas digitais de recolha e gestão de dados criminais permite analisar tendências e prevenir crimes de forma mais sistemática, considerando tanto a criminalidade objetiva quanto a experiência subjetiva da população.

No contexto de Angola, onde os sistemas de informação criminal podem ser incompletos ou desatualizados, a aplicação dessas teorias oferece uma abordagem científica para compreender a vitimização. Ao combinar a Teoria do Estilo de Vida e a Teoria da Vitimização Repetida com inquéritos de vitimização criminal e plataformas digitais, é possível:

- Identificar populações e locais mais vulneráveis, aumentando a eficácia das ações preventivas;
- Planejar políticas públicas baseadas em evidências, direcionando recursos humanos e materiais para áreas de maior risco;
- Reduzir a sensação de insegurança ao considerar tanto a criminalidade objetiva quanto a percepção da população;
- Avaliar impactos das políticas de segurança, permitindo ajustes contínuos com base em dados sistematizados.

Deste modo, as teorias de vitimização criminal oferecem fundamento teórico robusto para orientar a prevenção do crime e a proteção da população, alinhando análise científica, percepção social e planeamento estratégico.

1.2.3 Importância do uso de inquéritos de vitimização criminal

Os inquéritos de vitimização criminal são fundamentais para revelar a chamada cifra negra da criminalidade, correspondente aos crimes que não são denunciados às autoridades (Van Dijk, 2015).

Van Dijk (2015) afirma que "sem os inquéritos de vitimização, uma parte significativa da criminalidade permanece estatisticamente invisível" (p. 71).

O UNODC (2010) sustenta que estes instrumentos são indispensáveis para políticas públicas eficazes, ao declarar que "os dados de vitimização fornecem uma base de evidências para a prevenção do crime e para o planeamento da segurança" (p. 3).

Em contextos africanos e angolanos, marcados por níveis elevados de subnotificação, os inquéritos de vitimização permitem compreender as razões da não denúncia, como a desconfiança institucional e o medo de represálias (Alemika, 2015).

Alemika (2015) sublinha que "os inquéritos de vitimização são cruciais em contextos africanos onde os dados oficiais sobre criminalidade são incompletos ou pouco fiáveis" (p. 112).

Além disso, estes inquéritos contribuem para avaliar a percepção de segurança da população, elemento central para a legitimidade das políticas públicas e para o fortalecimento da confiança entre cidadãos e instituições de segurança (Jackson et al., 2017).

1.3 Evolução histórica da Percepção de Segurança

A percepção de segurança emergiu historicamente como uma preocupação social relacionada não apenas à ocorrência de crimes, mas também à sensação de proteção da população. Nos primórdios da criminologia moderna, a atenção estava centrada no infrator e no crime em si, enquanto a vítima e a experiência subjetiva de insegurança eram praticamente ignoradas (Fattah, 2010).

Garland (2001) observa que, com o desenvolvimento da "cultura do controlo", passou-se a enfatizar não apenas a criminalidade, mas também as ansiedades sociais e a percepção de risco dos cidadãos, reconhecendo que a sensação de insegurança pode gerar efeitos sociais significativos, independentemente das taxas de criminalidade objetivas.

Durante o século XX, especialmente nas áreas urbanas, cresceu o reconhecimento de que a experiência individual e coletiva da insegurança influencia comportamentos cotidianos, como evitar determinados locais, restringir mobilidade ou alterar hábitos sociais. Fattah (2010) reforça que a percepção de segurança e o medo do crime são tão socialmente construídos quanto os próprios crimes, evidenciando a importância de se estudar a insegurança como fenómeno social e psicológico.

Nos contextos contemporâneos, como o angolano, a percepção de segurança também reflete históricos de confiança institucional frágil, desigualdades sociais e experiências de vitimização, mostrando que compreender a percepção da população é essencial para políticas de prevenção mais eficazes (Jackson, Bradford, Stanko & Hohl, 2017).

1.3.1 Conceito de Percepção de Segurança e a sua classificação

Na criminologia, a percepção de segurança refere-se à avaliação subjetiva que os cidadãos fazem sobre a sua proteção face à criminalidade, considerando fatores cognitivos, emocionais e sociais (Jackson et al., 2017). Assim, dois cidadãos podem vivenciar a mesma realidade criminal, mas ter percepções de segurança distintas, dependendo de experiências pessoais, nível de confiança nas autoridades e características do bairro ou comunidade.

Etimologicamente, o termo segurança deriva do latim securitas, significando estado de tranquilidade, ausência de perigo ou proteção contra riscos (Cunha & Cintra, 2019). O termo percepção deriva do latim perceptio, que significa ato ou efeito de apreender ou compreender algo pelos sentidos ou pela mente, indicando um processo cognitivo e subjetivo de apreensão da realidade (Cunha & Cintra, 2019).

Jackson et al. (2017) reforçam que a confiança na polícia e a sensação de segurança são determinantes centrais da percepção de segurança pelos cidadãos, mostrando que medidas objetivas de criminalidade não são suficientes para explicar o medo do crime ou a insegurança sentida.

Portanto, a percepção de segurança integra indicadores objetivos e subjetivos, sendo um conceito multifacetado que combina experiências pessoais, influência social e confiança institucional, servindo de base para o desenho de políticas públicas, programas de prevenção e estratégias de planeamento urbano.

A literatura identifica diferentes tipos de percepção de segurança, que permitem analisar a experiência social da população:

- Percepção subjetiva individual: sensação pessoal de segurança ou vulnerabilidade em relação à criminalidade, influenciada por experiências de vitimização direta ou indireta, notícias e informações de vizinhos (Fattah, 2010).
- Percepção comunitária ou coletiva: avaliação agregada da segurança dentro de uma comunidade, refletindo coesão social, capital social e experiências compartilhadas de crime ou prevenção (Sampson, 2012).
- Percepção institucional: confiança na polícia, tribunais e outras instituições públicas de segurança, que afeta diretamente a sensação de proteção da população (Jackson et al., 2017).
- Percepção situacional: relacionada a contextos ou locais específicos, como ruas mal iluminadas, transportes públicos ou horários noturnos, que influenciam a avaliação do risco (Van Dijk, 2015).
- Percepção de risco: avaliação subjetiva da probabilidade de ser vítima de um crime, que pode ou não coincidir com indicadores objetivos de criminalidade.

- Percepção de eficácia das medidas de segurança: sentimento da população sobre a adequação e eficiência das políticas e ações implementadas pelas autoridades.
- Medo do crime: ainda que distinto, o medo do crime está estreitamente

relacionado à percepção de segurança e influencia comportamentos diários, mobilidade urbana, participação comunitária e apoio a políticas de prevenção (Alemika, 2015).

Fatores como experiência de vitimização pessoal ou de terceiros, cobertura mediática, histórico de violência local e desigualdade social desempenham papel central na formação da percepção de segurança. Por exemplo, bairros com maior presença policial podem apresentar baixa criminalidade real, mas ainda assim gerar alto nível de insegurança se houver desconfiança nas instituições (Jackson et al., 2017).

Compreender essas dimensões é fundamental para planeamento de políticas públicas de segurança, desenho urbano, programas de prevenção e avaliação de medidas de proteção, garantindo que as respostas da sociedade e do Estado considerem não apenas a criminalidade objetiva, mas também a experiência subjetiva de insegurança.

1.1 Evolução histórica do surgimento das plataformas digitais

Desde o início da revolução digital no século XX, a criação e evolução de plataformas digitais têm sido um processo contínuo e acumulativo na história tecnológica. A digitalização começou com a transição de formatos analógicos para formatos digitais, o que tornou possível a transmissão, processamento e armazenamento da informação de forma muito mais eficiente e confiável (Era da Informação, n.d.).

Na década de 1970, a invenção do microprocessador foi um marco inicial para o surgimento de tecnologias que viabilizariam plataformas digitais modernas. Segundo Acs, Song, Szerb, Audretsch e Komlósi (2022), "o microprocessador transformou o computador em algo acessível e escalável, gerando o desenvolvimento subsequente do computador pessoal, da internet, dos telemóveis inteligentes e da computação em nuvem" (p. X).

A popularização da internet e a evolução da Web constituíram outro momento histórico crucial. A transição de uma internet centrada em texto e estática (Web 1.0) para uma internet interativa e orientada ao utilizador (Web 2.0) permitiu o surgimento de sistemas que facilitam a interação, partilha de conteúdos e colaboração entre utilizadores, o que foi determinante para o surgimento de plataformas digitais tal como as conhecemos hoje (Web 2.0, n.d.).

Estudos na área da economia digital indicam que a ideia de plataformas não surgiu apenas com a tecnologia moderna, mas teve raízes em formas anteriores de mercados que facilitavam interacções e trocas entre agentes. A transformação que a internet proporcionou acelerou esses modelos e permitiu que empresas começassem a operar plataformas focadas na conexão entre diferentes utilizadores e serviços (Platform economy, n.d.).

De forma semelhante, fenómenos específicos como a aplicação das plataformas digitais em áreas científicas mostram que o conceito evoluiu ao longo das décadas, incorporando diferentes actores sociais incluindo académicos, governos e o sector privado – numa

transformação contínua que tem sido registada desde os anos 1990 (Plataformas digitais e actividade científica, 2021).

Assim, a evolução histórica das plataformas digitais é marcada por inovações tecnológicas profundas (como o microprocessador e a internet), por mudanças na forma como utilizadores interagem online (Web 2.0) e por transformações nos modelos de negócios e organização social que essas plataformas promovem.

1.1.1 Conceito de plataforma digital e a sua classificação

A palavra plataforma tem origem no francês plate-forme, que por sua vez provém da combinação de plat (chato, plano) e forme (forma), inicialmente significando uma superfície horizontal que serve de apoio ou suporte físico, como um palanque ou podium (Ciberdúvidas, 2021).

Com a revolução tecnológica e a transição para ambientes digitais, o conceito de plataforma foi transposto do espaço físico para o espaço digital, onde passou a designar estruturas que permitem a interacção e intermediação socio-económica em ambientes virtuais (Ha et al., 2024).

No contexto digital, pesquisadores definem plataforma digital como uma infraestrutura de software que facilita interações e transacções entre diferentes grupos de utilizadores, actuando como intermediário tecnológico entre produtores e consumidores de informação, bens ou serviços (Sørensen, Basole & De Reuver, 2018; Digital platform (infrastructure), n.d.).

A literatura científica reconhece que as plataformas digitais não são homogéneas, razão pela qual diversos autores propõem tipologias que permitem compreender as suas funções, estruturas e impactos sociais e económicos (Gawer, 2021).

De acordo com Gawer (2021), “as plataformas digitais podem ser entendidas como arquitecturas organizacionais distintas, cuja classificação depende do papel que desempenham na coordenação de actores, recursos e fluxos de informação” (p. 124).

Uma das tipologias mais consolidadas na literatura distingue as plataformas de transacção das plataformas de inovação, sendo esta classificação amplamente aceite no campo dos sistemas de informação e da economia digital (Evans & Schmalensee, 2016).

As plataformas de transacção são definidas como aquelas que “facilitam interacções directas entre dois ou mais grupos de utilizadores, reduzindo custos de pesquisa, coordenação e troca” (Evans & Schmalensee, 2016, p. 5).

Segundo Parker, Van Alstyne e Choudary (2016), este tipo de plataforma actua essencialmente como intermediário digital, organizando a oferta e a procura por meio de regras, algoritmos e mecanismos de governação.

Por outro lado, as plataformas de inovação caracterizam-se por fornecer uma base tecnológica sobre a qual terceiros podem desenvolver aplicações, serviços ou módulos

complementares, ampliando continuamente o valor do ecossistema digital (Tiwana, 2014).

Tiwana (2014) afirma que "uma plataforma de inovação é construída para permitir extensibilidade, de modo que actores externos possam criar soluções que se integrem à infraestrutura central" (p. 8).

A literatura mais recente acrescenta uma terceira categoria, designada plataformas de integração ou plataformas de dados, cujo foco principal reside na recolha, organização, processamento e interoperabilidade de grandes volumes de informação (de Reuver, Sørensen & Basole, 2018).

Segundo de Reuver et al. (2018), estas plataformas "funcionam como infra-estruturas digitais capazes de articular múltiplas fontes de dados, promovendo análises sistemáticas e suporte à tomada de decisão" (p. 127).

Outra classificação relevante considera o grau de controlo e governação, distinguindo plataformas centralizadas, descentralizadas e híbridas, o que influencia directamente a segurança da informação, a transparência e a autonomia dos utilizadores (Gillespie, 2018).

Gillespie (2018) sustenta que "a arquitectura de governação de uma plataforma define quem detém o poder de decisão sobre dados, regras de acesso e formas de utilização" (p. 23).

No contexto de plataformas digitais orientadas à gestão de dados sociais e criminais, a literatura destaca a predominância de plataformas de integração com características centralizadas, devido à necessidade de controlo institucional, fiabilidade da informação e protecção de dados sensíveis (Kitchin, 2021).

Kitchin (2021) sublinha que "plataformas digitais voltadas à gestão de dados públicos exigem estruturas robustas de governação, ética e segurança, dada a natureza sensível da informação tratada" (p. 64).

Assim, a tipologia das plataformas digitais permite compreender não apenas as suas funções técnicas, mas também os seus impactos sociais, institucionais e políticos, sendo um elemento essencial para o desenho de soluções digitais aplicadas à segurança pública e à análise de dados de vitimização criminal.

1.1.2 Plataformas digitais na recolha e gestão de dados criminais

As plataformas digitais configuram-se como infra-estruturas tecnológicas essenciais para a recolha e gestão de dados criminais, permitindo a integração, análise e cruzamento de informação de diferentes origens para fins de monitorização e tomada de decisão (Shan, 2026).

Num contexto de governação criminal transformada digitalmente, Shan (2026) argumenta que "as plataformas de governação abrangentes funcionam como infra-estruturas digitais que facilitam a agregação de informação, integração de dados multi-

fonte e avaliação de risco" (p. X), o que evidencia o papel destas plataformas na gestão sistemática dos dados.

A utilização de sistemas que centralizam dados em tempo real, como os chamados Real-Time Crime Centers, mostra a importância das plataformas digitais ao permitir que as forças de segurança unifiquem fluxos de vídeo, relatórios de incidentes e dados operacionais, ampliando a "consciência situacional e capacidades investigativas" (Real-Time Crime Center, n.d.).

Segundo pesquisas sobre ferramentas de informação para segurança pública, plataformas digitais que recolhem dados em tempo real e automatizam análises permitem às instituições policiais identificar padrões, detectar hotspots de criminalidade e coordenar respostas mais rápidas (Araghi et al., 2025).

A eficácia destas plataformas na recolha de dados também é reforçada tanto por estudos académicos quanto por exercícios práticos que demonstram a capacidade de integrar informação de utilizadores e sensores para produzir perfis incidentais e apoiar decisões operacionais imediatas (Crowdmapping, n.d.; Citizen app, n.d.).

Além disso, a literatura aponta que, ao digitalizar os processos tradicionais de recolha, armazenamento e análise de dados criminais, estas plataformas contribuem para reduzir o tempo de resposta e minimizar erros decorrentes de métodos manuais e não estruturados (Rewatkar et al., 2024).

Portanto, plataformas digitais representam ferramentas tecnológicas integradas que não só consolidam dados criminais e perceptivos, mas também potenciam a capacidade analítica e operacional das instituições envolvidas na prevenção e combate ao crime.

1.1.3 Importância das plataformas digitais para políticas públicas de segurança

A adopção de plataformas digitais tem sido reconhecida como um componente central na formulação e implementação de políticas públicas de segurança, uma vez que elevam significativamente a qualidade dos dados disponíveis para a definição de estratégias e medidas eficazes (Shan, 2026).

Shan (2026) enfatiza que "a governação através de plataformas representa uma reconfiguração paradigmática da resposta ao crime, deslocando-a de reacções reativas para abordagens preventivas fundamentadas em dados" (p. X), o que indica a importância destas plataformas na construção de políticas orientadas para a prevenção sustentada.

A integração de dados multi-fonte em plataformas digitais permite identificar tendências crimonológicas e perfis de risco mais precisos, promovendo assim medidas políticas que respondam não apenas a ocorrências específicas, mas também à dinâmica criminal subjacente (Shan, 2026).

Adicionalmente, plataformas digitais de reporte e análise de crime aumentam a participação dos cidadãos na segurança pública, pois permitem a comunicação directa

com as autoridades, o que pode levar a um aumento da taxa de denúncias e redução da subnotificação um factor crítico para políticas mais eficazes (Rewatkar et al., 2024).

A capacidade de processar grandes volumes de dados em tempo real e transformar essa informação em indicadores de desempenho operacional oferece aos decisores públicos uma base sólida para planear recursos, redesenhar programas e monitorizar resultados, contribuindo para uma governação mais inteligente e responsiva (Araghi et al., 2025).

Por fim, a literatura contemporânea sublinha que a integração de plataformas digitais no sistema de segurança pública possibilita uma coordenação interinstitucional mais forte, essencial para políticas que atravessam sectores como justiça, segurança comunitária e prevenção social tornando a abordagem de segurança pública mais holística e baseada em evidências.

1.1 Evolução histórica do surgimento das plataformas digitais

Desde o início da revolução digital no século XX, a criação e evolução de plataformas digitais têm sido um processo contínuo e acumulativo na história tecnológica. A digitalização começou com a transição de formatos analógicos para formatos digitais, o que tornou possível a transmissão, processamento e armazenamento da informação de forma muito mais eficiente e confiável (Era da Informação, n.d.).

Na década de 1970, a invenção do microprocessador foi um marco inicial para o surgimento de tecnologias que viabilizariam plataformas digitais modernas. Segundo Acs, Song, Szerb, Audretsch e Komlósi (2022), o microprocessador transformou o computador em algo acessível e escalável, gerando o desenvolvimento subsequente do computador pessoal, da internet, dos telemóveis inteligentes e da computação em nuvem.

A popularização da internet e a evolução da Web constituíram outro momento histórico crucial. A transição de uma internet centrada em texto e estática (Web 1.0) para uma internet interactiva e orientada ao utilizador (Web 2.0) permitiu o surgimento de sistemas que facilitam a interacção, partilha de conteúdos e colaboração entre utilizadores, o que foi determinante para o surgimento de plataformas digitais tal como as conhecemos hoje (Web 2.0, n.d.).

Estudos na área da economia digital indicam que a ideia de plataformas não surgiu apenas com a tecnologia moderna, mas teve raízes em formas anteriores de mercados que facilitavam interacções e trocas entre agentes. A transformação que a internet proporcionou acelerou esses modelos e permitiu que empresas começassem a operar

plataformas focadas na conexão entre diferentes utilizadores e serviços (Platform economy, n.d.).

Assim, a evolução histórica das plataformas digitais é marcada por inovações tecnológicas profundas (como o microprocessador e a internet), por mudanças na forma como utilizadores interagem online (Web 2.0) e por transformações nos modelos de negócios e organização social que essas plataformas promovem.

1.1.1 Conceito de plataforma digital e a sua classificação

A palavra *plataforma* tem origem no francês *plate-forme*, que por sua vez provém da combinação de *plat* (chato, plano) e *forme* (forma), inicialmente significando uma superfície horizontal que serve de apoio ou suporte físico (Ciberdúvidas, 2021). Com a revolução tecnológica, o conceito foi transposto do espaço físico para o espaço digital, onde passou a designar estruturas que permitem a interacção e intermediação socioeconómica em ambientes virtuais (Ha et al., 2024).

No contexto digital, pesquisadores definem plataforma digital como uma infraestrutura de software que facilita interacções e transacções entre diferentes grupos de utilizadores, actuando como intermediário tecnológico entre produtores e consumidores de informação, bens ou serviços (Sørensen, Basole & De Reuver, 2018).

A literatura científica reconhece que as plataformas digitais não são homogéneas, razão pela qual diversos autores propõem tipologias. Gawer (2021) sustenta que as plataformas digitais podem ser entendidas como arquitecturas organizacionais distintas, cuja classificação depende do papel que desempenham na coordenação de actores, recursos e fluxos de informação. Uma das tipologias mais consolidadas distingue as plataformas de transacção das plataformas de inovação (Evans & Schmalensee, 2016).

As plataformas de transacção facilitam interacções directas entre dois ou mais grupos de utilizadores, reduzindo custos de pesquisa, coordenação e troca (Evans & Schmalensee, 2016). Por outro lado, as plataformas de inovação caracterizam-se por fornecer uma base tecnológica sobre a qual terceiros podem desenvolver aplicações, serviços ou módulos complementares (Tiwana, 2014).

A literatura mais recente acrescenta uma terceira categoria, designada plataformas de integração ou plataformas de dados, cujo foco principal reside na recolha, organização, processamento e interoperabilidade de grandes volumes de informação (de Reuver, Sørensen & Basole, 2018). No contexto de plataformas digitais orientadas à gestão de dados sociais e criminais, a literatura destaca a predominância de plataformas de integração com características centralizadas, devido à necessidade de controlo institucional, fiabilidade da informação e protecção de dados sensíveis (Kitchin, 2021).

1.1.2 Plataformas digitais na recolha e gestão de dados criminais

As plataformas digitais configuram-se como infraestruturas tecnológicas essenciais para a recolha e gestão de dados criminais, permitindo a integração, análise e cruzamento de informação de diferentes origens para fins de monitorização e tomada de decisão (Shan, 2026). Num contexto de governação criminal transformada digitalmente, Shan (2026) argumenta que as plataformas de governação abrangentes funcionam como infraestruturas digitais que facilitam a agregação de informação, integração de dados multi-fonte e avaliação de risco.

A utilização de sistemas que centralizam dados em tempo real, como os chamados Real-Time Crime Centers, mostra a importância das plataformas digitais ao permitir que as forças de segurança unifiquem fluxos de vídeo, relatórios de incidentes e dados operacionais, ampliando a consciência situacional e capacidades investigativas (Real-Time Crime Center, n.d.).

Segundo pesquisas sobre ferramentas de informação para segurança pública, plataformas digitais que recolhem dados em tempo real e automatizam análises permitem às instituições policiais identificar padrões, detectar hotspots de criminalidade e coordenar respostas mais rápidas (Araghi et al., 2025). Além disso, ao digitalizar os processos tradicionais de recolha, armazenamento e análise de dados criminais, estas plataformas contribuem para reduzir o tempo de resposta e minimizar erros decorrentes de métodos manuais e não estruturados (Rewatkar et al., 2024).

1.5 Tecnologias Web: conceito e evolução

As tecnologias web representam um conjunto de ferramentas, linguagens e padrões que permitem o desenvolvimento de aplicações acessíveis através da internet. Inicialmente, a Web surgiu como um meio de disponibilização de informação estática, permitindo apenas a visualização de conteúdos sem interacção significativa por parte dos utilizadores. Segundo Tim Berners-Lee (2007), a Web não é apenas uma rede de máquinas, mas uma rede de pessoas que comunicam e interagem por meio do conhecimento compartilhado.

Com o avanço tecnológico, a Web evoluiu para o modelo Web 2.0, caracterizado pela participação activa dos utilizadores. De acordo com O'Reilly (2005), a Web 2.0 representou uma mudança de paradigma, onde os utilizadores passaram a ser produtores de conteúdo, transformando a Internet num espaço de inteligência colectiva. Esta evolução foi fundamental para o desenvolvimento de sistemas mais complexos, como a plataforma proposta neste trabalho, que permite aos cidadãos não apenas consultar informações, mas também registar denúncias, interagir com o sistema e contribuir com dados reais de vitimização criminal.

Actualmente, observa-se a transição para a Web 3.0, que incorpora tecnologias como inteligência artificial, análise de dados, personalização de conteúdos e sistemas inteligentes. Segundo Hendler, Shadbolt e Berners-Lee (2008), a Web Semântica visa estruturar a informação de modo que máquinas e humanos possam cooperar de forma mais eficaz. No contexto do presente trabalho, a plataforma integra funcionalidades inteligentes, como análise de dados de vitimização e um chatbot baseado em inteligência artificial.

1.1.3 Importância das plataformas digitais para políticas públicas de segurança

A adopção de plataformas digitais tem sido reconhecida como um componente central na formulação e implementação de políticas públicas de segurança. Shan (2026) enfatiza que a governação através de plataformas representa uma reconfiguração paradigmática da resposta ao crime, deslocando-a de reacções reactivas para abordagens preventivas fundamentadas em dados.

A integração de dados multi-fonte em plataformas digitais permite identificar tendências criminológicas e perfis de risco mais precisos, promovendo medidas políticas

que respondam não apenas a ocorrências específicas, mas também à dinâmica criminal subjacente (Shan, 2026). Adicionalmente, plataformas digitais de reporte e análise de crime aumentam a participação dos cidadãos na segurança pública, pois permitem a comunicação directa com as autoridades, o que pode levar a um aumento da taxa de denúncias e redução da subnotificação (Rewatkar et al., 2024).

A capacidade de processar grandes volumes de dados em tempo real e transformar essa informação em indicadores de desempenho operacional oferece aos decisores públicos uma base sólida para planear recursos, redesenhar programas e monitorizar resultados, contribuindo para uma governação mais inteligente e responsiva (Araghi et al., 2025). A literatura contemporânea sublinha que a integração de plataformas digitais no sistema de segurança pública possibilita uma coordenação interinstitucional mais forte, essencial para políticas que atravessam sectores como justiça, segurança comunitária e prevenção social.

1.4 Relação entre plataformas digitais, inquéritos de vitimização e percepção de segurança no planeamento de políticas públicas

As plataformas digitais têm-se tornado ferramentas essenciais na recolha, organização e análise de dados criminais, permitindo que informações complexas sobre criminalidade, vitimização e percepção de segurança sejam tratadas de forma sistemática e acessível (Van Dijk, 2015). Ao integrar os resultados de inquéritos de vitimização em plataformas digitais, é possível mapear áreas de maior vulnerabilidade, identificar grupos sociais mais expostos à criminalidade e detectar lacunas na segurança pública.

Fattah (2010) salienta que a vitimização secundária pode ser minimizada com sistemas digitais que centralizem informações, permitindo respostas mais rápidas e eficazes das autoridades. Jackson et al. (2017) destacam que a percepção de segurança está intimamente ligada à confiança na polícia e às experiências de vitimização, mostrando que o planeamento de políticas deve considerar tanto a criminalidade objectiva quanto a experiência subjectiva da população.

Alemika (2015) reforça que a utilização de dados confiáveis sobre vitimização e medo do crime em contextos africanos é fundamental para o planeamento estratégico de segurança pública. A integração entre plataformas digitais, inquéritos de vitimização e

indicadores de percepção de segurança oferece uma base científica para a formulação de políticas públicas, permitindo a tomada de decisão baseada em evidências, a melhoria na alocação de recursos, a monitorização de políticas em tempo real e o fortalecimento da confiança comunitária (Van Dijk, 2015; Fattah, 2010).

1.7 Sistemas de Informação aplicados à segurança pública

Os Sistemas de Informação (SI) são conjuntos organizados de componentes inter-relacionados que recolhem, processam, armazenam e distribuem informação para apoiar a tomada de decisão, a coordenação e o controlo numa organização (Laudon & Laudon, 2020). No domínio da segurança pública, os SI desempenham um papel crítico ao permitir a sistematização de dados criminais, a identificação de padrões e a geração de indicadores para o planeamento estratégico.

A aplicação de SI ao domínio criminal distingue-se pela sensibilidade dos dados tratados, pela multiplicidade de actores envolvidos (polícia, justiça, cidadãos, investigadores) e pela necessidade de equilibrar acessibilidade com segurança e privacidade. Kitchin (2021) sublinha que plataformas digitais voltadas à gestão de dados públicos exigem estruturas robustas de governação, ética e segurança, dada a natureza sensível da informação tratada.

No contexto do presente trabalho, a plataforma SafeAngola constitui um SI orientado ao domínio da vitimização criminal, concebido para apoiar quatro perfis de utilizadores com necessidades distintas: cidadãos (denúncias e consultas), investigadores (análise estatística e relatórios), polícia (gestão de ocorrências) e administradores (gestão completa do sistema). Esta arquitectura multi-perfil reflecte a prática recomendada na literatura de SI, que preconiza a diferenciação de acessos e funcionalidades conforme as necessidades e permissões de cada grupo de utilizadores (Laudon & Laudon, 2020).

A integração de inteligência artificial no sistema — através do chatbot pericial que combina análise estatística automática com modelos de linguagem natural — representa uma evolução significativa dos SI tradicionais. Esta abordagem alinha-se com as tendências contemporâneas de sistemas inteligentes de apoio à decisão, que não apenas armazenam e apresentam dados, mas transformam-nos em conhecimento acionável através de análise automatizada e interacção em linguagem natural.

Deste modo, a convergência entre tecnologia, dados de vitimização e percepção social transforma a forma como as políticas de segurança são concebidas, planeadas e avaliadas, promovendo respostas mais eficazes à criminalidade e maior sensação de protecção à população.

2.1 Desenvolvimento da plataforma

O desenvolvimento da plataforma digital foi orientado pela necessidade de criar um ambiente capaz de integrar dados de vitimização criminal e percepção de segurança, permitindo às instituições públicas e pesquisadores acesso facilitado a informações confiáveis e atualizadas. O processo de concepção envolveu etapas de análise de requisitos e modelagem, com foco na usabilidade, acessibilidade e adequação ao contexto urbano angolano.

A arquitetura da plataforma foi estruturada de modo a permitir a gestão eficiente de utilizadores (autoridades, investigadores e gestores públicos), o registo e atualização de dados de inquéritos, a sistematização de informações sobre incidentes e a geração de relatórios analíticos. Dessa forma, a plataforma proporciona uma visão integrada da vitimização criminal, permitindo identificar padrões de crime, áreas de maior risco e fatores de vulnerabilidade da população.

2.1.3 Metodologia utilizada para o desenvolvimento da plataforma *digital*

1.6 Metodologias ágeis de desenvolvimento de software

As metodologias ágeis surgiram como alternativa aos modelos tradicionais de desenvolvimento de software (como o modelo em cascata), que se mostravam rígidos e pouco adaptados a projectos com requisitos mutáveis. O Manifesto Ágil, publicado em 2001, estabeleceu quatro valores fundamentais: indivíduos e interacções acima de processos e ferramentas; software funcional acima de documentação extensa; colaboração com o cliente acima de negociação contratual; e resposta à mudança acima de seguir um plano (Beck et al., 2001).

Segundo Sommerville (2016), as metodologias ágeis caracterizam-se por ciclos curtos de desenvolvimento (iterações), entregas frequentes de software funcional, feedback contínuo dos utilizadores e capacidade de adaptação a mudanças de requisitos. Pressman e Maxim (2020) acrescentam que estas metodologias são particularmente adequadas para projectos onde os requisitos não estão completamente definidos no início, o que é frequente em projectos interdisciplinares como o presente.

1.6.1 Extreme Programming (XP)

O Extreme Programming (XP), proposto por Kent Beck (2004), é uma metodologia ágil que enfatiza a qualidade do software e a capacidade de resposta a mudanças nos requisitos. A XP fundamenta-se em cinco valores centrais: comunicação, simplicidade, feedback, coragem e respeito.

Entre as práticas fundamentais da XP destacam-se: o Planning Game (planeamento colaborativo das funcionalidades); o design simples (concepção da arquitectura mais simples que satisfaça os requisitos); a programação iterativa (construção incremental das funcionalidades); os testes contínuos (validação permanente do código); o refactoring (melhoria contínua da estrutura do código sem alterar o comportamento); e as entregas frequentes (disponibilização progressiva de módulos funcionais).

A escolha da XP para o presente projecto justifica-se pela natureza dinâmica e interdisciplinar do trabalho, que envolve múltiplos perfis de utilizadores (cidadãos, investigadores, polícia, administradores) com necessidades distintas e exige entregas incrementais de funcionalidades. A articulação entre a investigação criminológica (que produz dados e requisitos progressivamente) e o desenvolvimento de software (que materializa esses requisitos em funcionalidades) beneficia directamente dos ciclos curtos de feedback que a XP proporciona.

Segundo Fowler (2002), os frameworks encapsulam padrões de arquitectura que promovem reutilização de código e reduzem a complexidade do software. A combinação da XP com tecnologias modernas de desenvolvimento web (React, Next.js, Prisma) permite construir plataformas robustas mantendo a flexibilidade necessária para adaptações durante o ciclo de desenvolvimento.

Figura 1.

Extreme programming (Ciclo de desenvolvimento)

Fonte: https://artia.com/wp-content/uploads/2024/09/Imagens_Prancheta-1-01-780x780.png

O desenvolvimento da plataforma digital de análise de vitimização criminal e percepção de segurança adoptou a metodologia ágil **Extreme Programming (XP)**, seleccionada pela sua orientação a ciclos curtos de desenvolvimento, comunicação constante com os utilizadores, feedback rápido e adaptação contínua a mudanças de requisitos (Beck, 2004). A escolha desta metodologia justifica-se pela natureza dinâmica e interdisciplinar do projecto, que integra elementos das Ciências Criminais e da Engenharia Informática, exigindo flexibilidade na implementação e validação contínua das funcionalidades.

Além disso, o sistema desenvolvido envolve múltiplos perfis de utilizadores — cidadão, investigador, polícia e administrador — cada um com necessidades específicas, o que torna essencial uma abordagem iterativa que permita ajustes frequentes e melhoria contínua do sistema. A presença de componentes avançados, como o chatbot inteligente e os módulos de análise estatística, reforça ainda mais a necessidade de uma metodologia adaptativa como a XP.

A metodologia utilizada no desenvolvimento baseou-se em princípios ágeis, mais especificamente na abordagem **Extreme Programming (XP)**, escolhida pela sua flexibilidade e capacidade de adaptação a mudanças frequentes. Essa metodologia orientou o trabalho em ciclos curtos de desenvolvimento, permitindo a revisão constante das funcionalidades e o aprimoramento contínuo do sistema.

A escolha dessa abordagem justifica-se pela natureza dinâmica do projeto, que exige respostas rápidas às necessidades dos usuários (autoridades, investigadores e cidadãos)

e a entrega progressiva de funcionalidades que garantam o acompanhamento efetivo dos dados de vitimização criminal.

2.1.3.1 Características, vantagens e desvantagens da metodologia

A metodologia Extreme Programming (XP) caracteriza-se pela sua natureza ágil, iterativa e colaborativa, promovendo a entrega contínua de software funcional através de pequenos ciclos de desenvolvimento. Entre as suas principais características destacam-se:

- Comunicação constante entre os membros da equipa;
- Feedback rápido dos usuários sobre a utilidade da plataforma;
- Refinamento contínuo das funcionalidades;
- Simplicidade das soluções aplicadas à gestão de dados criminais.

Entre as vantagens da XP estão a alta qualidade do produto final, a rápida adaptação a mudanças de requisitos e a forte integração com as necessidades dos utilizadores. Entre as desvantagens, destacam-se a necessidade de grande comprometimento da equipe e dos usuários, a dificuldade de aplicação em projetos de grande escala e a dependência de comunicação eficaz.

2.1.3.2 Princípios e valores da XP aplicados ao projecto

A metodologia XP fundamenta-se em cinco valores centrais: comunicação, simplicidade, feedback, coragem e respeito (Beck, 2004). No contexto do presente projecto, estes valores foram aplicados da seguinte forma:

- Comunicação: houve uma interacção constante entre a equipa de desenvolvimento e os potenciais utilizadores do sistema, permitindo validar requisitos relacionados à recolha de dados de vitimização, análise estatística e funcionalidades do chatbot inteligente;
- Simplicidade: o sistema foi desenvolvido priorizando funcionalidades essenciais, como registo de denúncias, visualização de dados e geração de relatórios, evitando complexidade desnecessária nas primeiras versões;
- Feedback: foram realizadas entregas incrementais de módulos, como autenticação, dashboards e chatbot, permitindo avaliar o funcionamento do sistema e introduzir melhorias com base nos resultados obtidos;
- Coragem: durante o desenvolvimento, decisões de design e implementação foram revistas sempre que necessário, especialmente na optimização dos módulos de análise estatística e integração com inteligência artificial;
- Respeito: foi mantido um ambiente colaborativo, respeitando as contribuições dos membros da equipa e dos participantes envolvidos na recolha de dados.

2.1.3.3 Fases do ciclo de desenvolvimento

O desenvolvimento seguiu as fases típicas da XP, adaptadas ao contexto académico e tecnológico do projecto:

1. Planeamento (Planning Game)

Nesta fase, foram identificadas e priorizadas as funcionalidades do sistema (user stories), com base nos requisitos levantados junto dos diferentes actores do sistema. Foram definidos módulos como:

- registo e autenticação de utilizadores;
- envio e gestão de denúncias;
- análise estatística dos dados;
- visualização de dashboards;
- integração do chatbot inteligente.

A priorização considerou o impacto de cada funcionalidade na análise da vitimização criminal e no apoio à tomada de decisão.

2. Design Simples

A arquitectura do sistema foi concebida de forma modular, com separação entre:

frontend

O frontend foi desenvolvido com tecnologias modernas, garantindo uma interface interativa, responsiva e orientada à visualização de dados criminais.

Foram utilizadas as seguintes ferramentas:

- Framework: Next.js (versão 14 – App Router)
- Biblioteca base: React
- Linguagem: TypeScript
- Estilização: Tailwind CSS
- Componentes UI: Shadcn UI (baseada em Radix UI)
- Ícones: Lucide
- Gráficos: Recharts e Chart.js
- Animações: Framer Motion e Tailwind Animate
- Gestão de temas: Next Themes (modo claro/escuro)
- Chart.js – Criação de gráficos dinâmicos (barra, pizza, linha);

Backend (Processamento e Lógica do Sistema)

O backend do sistema foi desenvolvido com uma abordagem híbrida, combinando tecnologias de JavaScript (Node.js) para gestão da aplicação web e Python para análise científica e estatística dos dados criminais.

Camada de Aplicação Web (Node.js)

Esta camada é responsável pela gestão da lógica do sistema, comunicação com o frontend e manipulação da base de dados.

Foram utilizadas as seguintes tecnologias:

- **Ambiente de execução:** Node.js
- **Framework de API:** Next.js (Route Handlers / API Routes)
- **ORM (Gestão de Dados):** Prisma
- **Base de Dados:** SQLite
- **Autenticação:** BcryptJS
- **Envio de E-mails:** Nodemailer
- **Processamento de ficheiros:** ExcelJS
- **Validação de dados:** Zod
- **Python** – Linguagem principal para processamento científico e análise de dados;
- **Pandas** – Manipulação e tratamento de dados (pré-processamento);
- **SciPy (scipy.stats)** – Execução de testes estatísticos (Correlação, Qui-quadrado, ANOVA, Teste t);
- **Integração com IA (Google Gemini 2.5 Flash)** – Processamento de linguagem natural e geração de respostas inteligentes;

Além disso, foi adoptada uma estrutura em camadas para suportar o chatbot inteligente, incluindo pré-processamento de dados, motor estatístico e integração com inteligência artificial.

3. Codificação

A implementação foi realizada de forma iterativa, utilizando:

- **TypeScript** para maior segurança e organização do código;
- **Componentes reutilizáveis** (shadcn-ui, Radix UI) para padronização da interface;
- **Prisma ORM** para abstração da base de dados;
- **Bibliotecas especializadas** como Recharts e ExcelJS para análise e visualização de dados.

Nesta fase, também foi implementado o módulo de inteligência artificial, responsável por transformar dados de inquéritos em análises interpretativas.

4. Testes

Foram realizados testes contínuos para garantir a qualidade do sistema, incluindo:

- validação de formulários de denúncia;
- testes de autenticação e segurança;
- verificação da importação de dados via Excel;
- validação dos cálculos estatísticos (correlações, testes de hipóteses);
- testes de funcionamento do chatbot;
- Validação na parte das notificações.

Esses testes permitiram assegurar a integridade dos dados e a fiabilidade das análises geradas.

5. Entregas Incrementais

O sistema foi desenvolvido de forma modular, sendo os seus componentes disponibilizados progressivamente, o que permitiu validar cada funcionalidade antes da integração final. Com base na análise completa da estrutura de ficheiros e funcionalidades do projeto, a plataforma é composta pelos seguintes módulos principais:

1. Módulo de Autenticação e Gestão de Acessos
   Responsável pelo registo de utilizadores, login seguro e recuperação de palavra-passe. Implementa também diferentes níveis de acesso (Administrador, Investigador, Autoridade Policial e Cidadão), garantindo controlo e segurança no uso da plataforma.
2. Módulo de Reporte e Ocorrências (Denúncias)
   Permite aos cidadãos registar denúncias de forma segura. Inclui funcionalidades para gestão e monitorização de incidentes por parte das autoridades competentes.
3. Módulo de Gestão e Visualização de Dados
   Integra ferramentas para inserção manual de dados e importação em massa via Excel, bem como mecanismos de consulta com filtros avançados para análise de informações recolhidas.
4. Módulo de Dashboard e Estatísticas
   Disponibiliza um painel de controlo dinâmico adaptado ao perfil do utilizador, com visualização de métricas principais e indicadores relevantes em tempo real.
5. Módulo de Análise Estatística e Gráficos
   Responsável pela geração de gráficos dinâmicos (barra, pizza, linha) com base em múltiplos indicadores, permitindo o cruzamento de dados por diferentes variáveis como género, idade e localização.
6. Módulo de Inteligência Artificial (Chatbot)
   Oferece uma interface conversacional que permite aos utilizadores obter informações e estatísticas em tempo real através de linguagem natural.
7. Módulo de Geração de Relatórios
   Permite a criação automática de relatórios com base nos dados recolhidos e nas análises realizadas, facilitando a tomada de decisão.
8. Módulo de Administração do Sistema
   Responsável pela gestão de utilizadores, controlo de permissões e manutenção da integridade e segurança da base de dados.
9. Módulo de Comunicação e Notícias
   Inclui funcionalidades para publicação de conteúdos informativos, campanhas de sensibilização e divulgação de materiais educativos para a comunidade.

Essa abordagem permitiu validar cada componente antes da integração final.

2.1.3.4 Vantagens e limitações da XP no contexto do projecto

Entre as principais vantagens da utilização da metodologia XP neste projecto, destacam-se:

- **Melhoria da qualidade do sistema**, proporcionada pelo feedback contínuo e pela identificação precoce de falhas;
- **Elevada capacidade de adaptação a mudanças nos requisitos**, permitindo ajustes rápidos conforme as necessidades do projecto;
- **Desenvolvimento centrado no utilizador**, assegurando o alinhamento entre as expectativas dos utilizadores (autoridades e investigadores) e as funcionalidades implementadas;
- **Entrega incremental de módulos**, facilitando a validação progressiva do sistema e a organização eficiente dos dados;
- **Integração eficaz entre componentes tecnológicos e científicos**, nomeadamente estatística e inteligência artificial;
- **Apoio à tomada de decisões baseadas em evidências**, através da disponibilização de dados organizados e analisados.

Por outro lado, algumas limitações foram identificadas:

- necessidade de elevado comprometimento da equipa;
- dificuldade de aplicar algumas práticas da XP, como programação em par, devido ao contexto académico;
- dependência de comunicação constante para garantir alinhamento do projecto.

A adopção da metodologia XP mostrou-se adequada ao desenvolvimento da plataforma de vitimização criminal, permitindo conciliar rigor científico, flexibilidade tecnológica e foco nas necessidades dos utilizadores. A abordagem incremental e iterativa facilitou a integração de funcionalidades complexas, como a análise estatística e o chatbot inteligente, contribuindo para a construção de um sistema robusto, adaptável e orientado à tomada de decisão em segurança pública.

2.1.4 Linguagens de Programação e Frameworks Utilizadas

O desenvolvimento da plataforma digital de análise de vitimização criminal baseia-se na utilização de tecnologias modernas de desenvolvimento web, que permitem a construção de sistemas robustos, escaláveis e interactivos.

1.7.1 React

Figura 2.

React

Fonte: https://upload.wikimedia.org/wikipedia/commons/a/a7/React-icon.svg

O React é uma biblioteca JavaScript desenvolvida pelo Facebook para a construção de interfaces interativas e reativas. Segundo Banks e Porcello (2017), "o React permite a criação de componentes reutilizáveis, o que facilita a manutenção e escalabilidade de aplicações web complexas" (p. 15).

Baseado no conceito de componentização, o React permite dividir a interface em partes independentes e reutilizáveis, tornando o desenvolvimento mais organizado e eficiente. Além disso, o uso do Virtual DOM possibilita atualizações rápidas e otimizadas da interface, melhorando o desempenho da aplicação.

No contexto da plataforma, o React proporciona uma experiência de usuário fluida e responsiva, essencial para interações em tempo real. Adicionalmente, sua grande comunidade e vasta documentação garantem suporte contínuo e acesso a diversas ferramentas complementares, reforçando sua adoção no desenvolvimento web moderno.

1.7.2 Next.js

Figura 3.

Fonte: https://upload.wikimedia.org/wikipedia/commons/8/8e/Nextjs-logo.svg

O Next.js é um framework baseado em React que oferece renderização do lado do servidor e geração estática de páginas, melhorando o desempenho e a indexação em motores de busca. Conforme Mezzetti (2020), "o Next.js combina a flexibilidade do React com funcionalidades avançadas para aplicações web modernas, como SSR, SSG e roteamento automático" (p. 22).

Este framework permite o desenvolvimento de aplicações mais rápidas e eficientes, ao reduzir o tempo de carregamento das páginas e otimizar a experiência do utilizador. Além disso, o sistema de roteamento automático e a organização baseada em ficheiros tornam o desenvolvimento mais simples e estruturado.

Para a plataforma proposta, o Next.js garante páginas rápidas, escaláveis e de fácil manutenção. A sua integração com o ecossistema React e suporte a boas práticas modernas tornam-no uma escolha adequada para aplicações web robustas e orientadas a desempenho.

.

1.7.3 Tailwind CSS

Figura 4.

Fonte: https://upload.wikimedia.org/wikipedia/commons/d/d5/Tailwind_CSS_Logo.svg

O Tailwind CSS é um framework de utilitários CSS que permite estilizar elementos diretamente no HTML, acelerando o desenvolvimento de interfaces modernas. De acordo com O'Reilly (2021), "Tailwind promove a criação de layouts consistentes sem a necessidade de escrever CSS personalizado em excesso" (p. 18).

Baseado numa abordagem utilitária, o Tailwind CSS oferece classes pré-definidas que permitem aplicar estilos de forma rápida e consistente, reduzindo a duplicação de código e facilitando a manutenção. Essa abordagem contribui para maior produtividade no desenvolvimento e melhor organização visual das aplicações.

Na plataforma, o Tailwind CSS facilita a padronização visual e o desenvolvimento rápido de componentes responsivos. Além disso, permite criar interfaces modernas e adaptáveis a diferentes dispositivos, garantindo uma melhor experiência do utilizador.

1.7.4 shadcn-ui + Radix UI

Figura 5.

Fonte: https://avatars.githubusercontent.com/u/49277992?s=280&v=4

O shadcn-ui, em conjunto com o Radix UI, oferece componentes reutilizáveis de alta qualidade, garantindo consistência e acessibilidade na construção de interfaces modernas. Segundo a documentação oficial (2023), "Radix UI fornece primitives acessíveis enquanto shadcn-ui agrega estilos e padrões modernos".

Esta combinação permite o desenvolvimento de interfaces robustas e bem estruturadas, com foco na acessibilidade e usabilidade. Enquanto o Radix UI fornece a base funcional e acessível dos componentes, o shadcn-ui adiciona uma camada de estilização moderna e flexível, facilitando a personalização.

Na plataforma, essa integração possibilita a criação de interfaces profissionais, consistentes e de fácil manutenção, sem comprometer a experiência do utilizador. Além disso, contribui para acelerar o desenvolvimento e garantir boas práticas no design de sistemas interativos.

1.7.5 Node.js

Figura 6.

Fonte: https://upload.wikimedia.org/wikipedia/commons/d/d9/Node.js_logo.svg

O Node.js é um ambiente de execução JavaScript no servidor que permite construir aplicações escaláveis e de alto desempenho. Como afirmam Tilkov e Vinoski (2010), "Node.js destaca-se pelo seu modelo de I/O não bloqueante, que é ideal para aplicações em tempo real e com grande volume de dados" (p. 9).

Com a sua arquitetura assíncrona baseada em eventos, o Node.js possibilita que múltiplas operações sejam processadas simultaneamente sem bloquear o servidor, aumentando a eficiência e a capacidade de resposta. Esse modelo é particularmente vantajoso para sistemas que exigem interações em tempo real e manipulação contínua de dados.

Para o backend da plataforma, o Node.js garante eficiência na comunicação entre clientes e servidor, suportando aplicações robustas e escaláveis. Além disso, sua vasta comunidade e ecossistema de pacotes NPM oferecem suporte contínuo e ferramentas para acelerar o desenvolvimento de soluções complexas.

1.7.6 Prisma ORM

Figura 7.

Fonte: https://www.prisma.io/images/brand/prisma-logo-light.svg

O Prisma é uma ferramenta de mapeamento objeto-relacional (ORM) que simplifica a interação com bases de dados. Conforme S. Chen (2021), "Prisma permite a definição de esquemas tipados e consultas seguras, reduzindo erros e aumentando a produtividade" (p. 12).

Com sua abordagem tipada e geração automática de consultas, o Prisma oferece maior segurança e consistência na manipulação de dados, prevenindo erros comuns em SQL manual. Além disso, facilita migrações e versionamento do esquema da base de dados, tornando o desenvolvimento mais organizado e confiável.

Na plataforma, o Prisma permite gerir de forma eficiente a base de dados SQLite, tornando operações complexas mais simples, seguras e padronizadas. Essa integração contribui para maior produtividade da equipe de desenvolvimento e garante manutenção mais ágil e confiável dos dados.

1.7.7 Docker

Figura 8.

Fonte: https://www.docker.com/wp-content/uploads/2022/03/Moby-logo.png

O Docker é uma plataforma de containerização que garante a padronização e portabilidade de ambientes de desenvolvimento. De acordo com Merkel (2014), “containers isolam aplicações e suas dependências, promovendo consistência entre desenvolvimento, teste e produção” (p. 7).

Ao utilizar containers, o Docker permite que cada aplicação e suas dependências sejam empacotadas de forma isolada, eliminando problemas de compatibilidade entre diferentes ambientes. Isso proporciona maior confiabilidade, facilidade na distribuição e consistência no ciclo de desenvolvimento, teste e implantação.

Para a plataforma, o Docker assegura que todos os módulos funcionem corretamente independentemente do ambiente, facilitando a manutenção, escalabilidade e atualização dos serviços. Além disso, sua ampla adoção no mercado e comunidade ativa garantem suporte contínuo e acesso a ferramentas complementares.

1.7.8 Recharts

Figura 9.

Fonte: https://recharts.org/img/recharts.svg

O Recharts é uma biblioteca para geração de gráficos estatísticos em React, permitindo a visualização de dados de forma clara e interativa. Segundo a documentação oficial (2023), “Recharts é construído com componentes React, facilitando a integração em projetos modernos e personalizáveis”.

Baseado em componentes reutilizáveis, o Recharts possibilita criar gráficos dinâmicos e responsivos de maneira simples, permitindo personalização de estilos, tipos de gráficos e interatividade. Essa abordagem facilita a manutenção e atualização das visualizações conforme os requisitos do projeto evoluem.

Na plataforma, o Recharts auxilia no monitoramento de métricas e análise de desempenho de usuários e sistemas, oferecendo insights visuais precisos e acessíveis. Além disso, sua integração nativa com React garante compatibilidade e consistência com o restante da aplicação.

1.7.15 Visual studio code

Figura 16.

Fonte: https://icons.veryicon.com/png/o/business/vscode-program-item-icon/vscode.png

O Visual *Studio Code* (VS *Code*) é um editor de código amplamente adoptado pela sua leveza e extensibilidade. Segundo Han et al. (2017), "o VS *Code* destaca-se por oferecer recursos avançados de edição sem comprometer o desempenho" (p. 15). Essa característica torna-o ideal para o desenvolvimento ágil da plataforma.

Outro aspecto importante são as suas extensões. Para Rees (2018), "o ecossistema de *plugins* do VS *Code* permite que cada desenvolvedor personalize o ambiente de acordo com as suas necessidades" (p. 40). Isso facilita a integração com PHP, *JavaScript*, *MySQL* e outras tecnologias da plataforma.

Além disso, a sua *interface* simplificada contribui para maior produtividade. De acordo com Brown (2019), "a curva de aprendizagem do VS *Code* é baixa, mas a sua capacidade de adaptação a projectos complexos é elevada" (p. 27). Isso garante uma melhor organização e manutenção do código do sistema.

1.7.16 Python

Figura 17.

Fonte: https://www.python.org/static/community_logos/python-logo.png

Python é uma linguagem de programação de alto nível, interpretada e de fácil leitura, amplamente usada para análise de dados e desenvolvimento científico. Segundo Lutz (2013), "Python combina simplicidade e poder, sendo ideal para prototipagem rápida e scripts de processamento de dados" (p. 22).

No projeto, Python é usado no backend para processar os dados brutos de vitimização, criar índices criminais e gerar estatísticas periciais.

Além disso, Python integra bibliotecas científicas como pandas, numpy e scipy, permitindo cálculos estatísticos complexos e manipulação de grandes volumes de dados.

1.7.17 Pandas

Figura 18.

Fonte: https://pandas.pydata.org/static/img/pandas_mark.svg

O Pandas é uma biblioteca Python voltada para manipulação e análise de dados, oferecendo estruturas como DataFrames para fácil manuseio de tabelas. Conforme McKinney (2010), “Pandas permite limpeza, filtragem e transformação de grandes conjuntos de dados de maneira eficiente” (p. 35).

Na plataforma, Pandas é utilizado no pré-processamento, convertendo respostas qualitativas em dados quantitativos e criando índices compostos como Idx_Inseguranca e Idx_Confianca_Institucional.

Também possibilita operações de agrupamento, filtragem e exportação de dados para análise posterior pelo Motor Pericial ou visualização no frontend.

1.7.18 SciPy

Figura 19.

Fonte: https://studyopedia.com/python-libraries/scipy-library/

O SciPy é uma biblioteca Python de computação científica que fornece funções para estatística, álgebra linear, integração e otimização. De acordo com Virtanen et al. (2020), “SciPy oferece ferramentas robustas para análise estatística e validação de hipóteses” (p. 12).

Na plataforma, o SciPy é utilizado no Motor Pericial para cálculos como Correlação de Pearson, Teste Qui-Quadrado, ANOVA e Teste t-Student.

Isso garante que as análises de vitimização sejam estatisticamente significativas, permitindo interpretações confiáveis para estudos criminais.

1.7.19 Chart.js

Figura 20.

Fonte: https://www.chartjs.org/media/logo-title.svg

O Chart.js é uma biblioteca JavaScript para criação de gráficos interativos em páginas web. Segundo documentação oficial (2023), “Chart.js facilita a visualização de dados de forma clara, atraente e personalizável”.

No projeto, Chart.js é usado no frontend para exibir métricas criminais, índices e tendências derivadas do Motor Pericial.

Isso permite que estudantes e peritos explorem os dados visualmente, ajudando na análise de padrões e hotspots de criminalidade.

1.7.20 Google Gemini (IA)

Figura 21.

Fonte: https://gemini.google.com/app

O Google Gemini é uma plataforma de modelos de IA avançados para Processamento de Linguagem Natural. De acordo com a documentação oficial (2023), “Gemini interpreta dados complexos e gera respostas contextualizadas sem recorrer a informações externas”.

Na plataforma, Gemini processa o “Mega-Contexto” JSON gerado pelo Motor Pericial e responde às consultas dos usuários de forma precisa e orientada.

Também garante que a IA atue como um perito forense, respeitando a regra de não usar conhecimentos externos e trabalhando apenas com os dados fornecidos.

Bibliotecas complementares: ExcelJS para importação e exportação de ficheiros Excel; bcryptjs para encriptação de senhas; nodemailer para envio de emails automáticos; react-hook-form para gestão de formulários; @tanstack/react-query para gestão de estado e consumo de APIs; e next-themes para controlo de temas (claro/escuro).

.5.2 Desenvolvimento do Chatbot Inteligente de Vitimização Criminal

Um dos principais diferenciais da plataforma desenvolvida é a integração de um chatbot inteligente, concebido para auxiliar na análise de dados de vitimização criminal e percepção de segurança. O chatbot está disponível na interface do sistema e permite ao

utilizador consultar dados de vitimização, gerar relatórios automaticamente, obter análises estatísticas e fazer perguntas relacionadas à segurança pública.

O sistema foi desenvolvido com base numa arquitectura dividida em quatro camadas: (1) Pré-processamento de Dados, responsável pela limpeza, organização e transformação dos dados recolhidos nos inquéritos, incluindo a conversão de dados qualitativos em quantitativos e a criação de variáveis analíticas; (2) Motor Pericial, que constitui o núcleo científico do sistema, aplicando métodos estatísticos como correlação de Pearson, teste Qui-Quadrado, ANOVA e teste t-Student para validar hipóteses relacionadas com vitimização, percepção de segurança e comportamento das vítimas; (3) Integração com Inteligência Artificial, onde o sistema gera um contexto estatístico completo e o envia ao modelo de IA (Google Gemini), que responde com base exclusivamente nos dados fornecidos, garantindo rigor científico; e (4) Interface e Segurança, responsável pela interacção com o utilizador através de uma interface moderna e intuitiva, com sistema de autenticação e protecção de dados.

2.1.5 Desenvolvimento do Chatbot Inteligente de Vitimização Criminal

Um dos principais diferenciais da plataforma desenvolvida é a integração de um chatbot inteligente, concebido para auxiliar na análise de dados de vitimização criminal e percepção de segurança.

O chatbot está disponível na interface do sistema (dashboard) e permite ao utilizador:

- Consultar dados de vitimização;
- Gerar relatórios automaticamente;
- Obter análises estatísticas;
- Fazer perguntas relacionadas à segurança pública em função dos dados obtidos.

2.1.5.1 Arquitectura do Sistema Inteligente

O sistema foi desenvolvido com base numa arquitectura modular, organizada em quatro camadas principais, permitindo a integração entre análise estatística, processamento de dados e inteligência artificial aplicada às Ciências Criminais.

1. Pré-processamento de Dados

Esta camada é responsável pela limpeza, organização e transformação dos dados recolhidos nos inquéritos, garantindo a sua adequação para análise científica.

Inclui as seguintes operações:

- Conversão de dados qualitativos em quantitativos através de **mapeamento ordinal** (ex: níveis de segurança convertidos em valores numéricos);
- Criação de variáveis analíticas e indicadores compostos, tais como:
    - Índice de Insegurança (percepção diurna e nocturna);
    - Índice de Confiança Institucional (presença, eficácia e confiança na polícia);
- Extração de factores de risco, transformando respostas em variáveis binárias (ex: medo, falta de iluminação, desemprego);
- Preparação e normalização dos dados para análise estatística e processamento pelo motor pericial.

2. Motor Pericial (Análise Estatística)

Este módulo constitui o núcleo científico do sistema, sendo responsável pela validação de hipóteses criminais com base em métodos estatísticos reconhecidos.

As principais técnicas utilizadas incluem:

- **Correlação de Pearson (r)** – análise da relação entre variáveis (ex: presença policial vs insegurança);
- **Teste Qui-Quadrado (χ^2)** – verificação de associação entre variáveis categóricas (ex: género vs denúncia);
- **ANOVA e Teste t-Student** – comparação de médias entre diferentes grupos (ex: bairros);

Adicionalmente, este módulo:

- Calcula níveis de significância estatística (p-value < 0.05);
- Gera estruturas de dados analíticos (contexto estatístico em formato estruturado);
- Permite análises como:
    - vitimização criminal;
    - percepção de segurança;
    - comportamento das vítimas;
    - identificação de padrões e tendências criminais.

3. Integração com Inteligência Artificial

O sistema integra um modelo de Inteligência Artificial que actua como um **perito criminal digital**, permitindo consultas em linguagem natural com base em dados reais.

O funcionamento ocorre da seguinte forma:

1. O Motor Pericial gera um **contexto estatístico completo** (em formato estruturado, como JSON);
2. Esse contexto é enviado ao modelo de IA juntamente com a questão do utilizador;

3. A IA responde exclusivamente com base nos dados fornecidos, respeitando uma lógica de análise científica controlada.

Além disso, a IA suporta diferentes tipos de consultas:

- **Descritivas** – apresentação de frequências e percentagens de crimes;
- **Comparativas** – análise entre grupos (ex: género, idade);
- **Relacionais** – interpretação de correlações e significância estatística;
- **Geográficas** – identificação de padrões por bairro (hotspots criminais).

Este modelo garante rigor analítico e evita inferências externas não fundamentadas.

4. Interface e Segurança

Esta camada é responsável pela interacção entre o utilizador e o sistema, assegurando acessibilidade, usabilidade e protecção da informação.

Inclui:

- Interface moderna, interactiva e orientada ao utilizador;
- Sistema de autenticação e gestão de utilizadores;
- Controlo de acessos baseado em perfis (roles);
- Visualização de dados através de dashboards e gráficos dinâmicos;
- Protecção e integridade dos dados armazenados.

Tabela 1.

Funcionalidades do chatboot

Tipo de Consulta	Funcionalidade
Descritiva	Quantificação de crimes
Comparativa	Análise por género, idade, etc.
Relacional	Relação entre factores (ex: iluminação vs crime)
Geográfica	Identificação de zonas mais perigosas

Fonte: Elaborado pela autora, 2026

CAPÍTULO II: ANÁLISE DE DADOS E DESENVOLVIMENTO DA PLATAFORMA DIGITAL

No presente trabalho, será representado em tabelas todos os resultados obtidos através da aplicação do inquérito de vitimização criminal e percepção de segurança no município da Samba situado na cidade de Luanda com o objectivo de esclarecer melhor o tema em análise.

2.1 Apresentação dos dados sociodemográficos da amostra

Tabela 1 – Distribuição dos inquiridos por faixa etária

Faixa Etária	Frequência (n)	Percentagem (%)
18–25 anos	159	30,5%
26–35 anos	116	22,2%
36–45 anos	140	26,8%
46–55 anos	53	10,2%
Mais de 55 anos	54	10,3%
Total	522	100%

Análise Quantitativa:

A amostra é maioritariamente jovem com 30,5%, seguido pela faixa etária de 36–45 anos (26,8%). Os grupos acima de 45 anos representam, em conjunto, cerca de 20% da amostra, indicando uma população relativamente jovem no contexto estudado.

Análise Qualitativa:

O predomínio de jovens adultos sugere uma comunidade em fase ativa de consolidação familiar e profissional. Este perfil pode estar associado a maior mobilidade, uso intenso do espaço público e rotinas que os tornam mais expostos a determinados tipos de criminalidade, como roubos e furtos. Paralelamente, a baixa representatividade de idosos (>55 anos: 10,3%) pode indicar uma migração seletiva ou dinâmicas familiares que influenciam a percepção de segurança, pois os jovens podem priorizar questões de policiamento imediato, enquanto os riscos de grupos etários mais velhos (como isolamento ou fraudes) podem estar sub-representados na percepção coletiva.

Tabela 2 – Distribuição dos inquiridos por Gênero

Gênero	Frequência (n)	Percentagem (%)
Feminino	266	51,0%
Masculino	256	49,0%
Total	522	100%

Análise Quantitativa:

A distribuição por gênero é praticamente equitativa, com uma ligeira predominância feminina (51% contra 49%), assegurando uma representatividade balanceada de ambos os sexos na análise.

Interpretação Qualitativa:

Este equilíbrio é positivo para a representatividade da amostra. Contudo, feminino pode refletir um maior engajamento das mulheres em pesquisas comunitárias ou uma maior preocupação com temas de segurança no bairro. Esta característica qualifica a amostra como particularmente sensível a questões de segurança de gênero, podendo influenciar percepções sobre violência doméstica ou assédio, e conecta-se possivelmente com a percepção de baixa cooperação vizinha pois as mulheres, frequentemente sobrecarregadas com responsabilidades domésticas, podem experienciar maior isolamento social.

Tabela 3 – Distribuição dos inquiridos por Ocupação

Ocupação	Frequência (n)	Percentagem (%)
Trabalha	321	61,5%
Estuda	119	22,8%
Trabalha e Estuda	34	6,5%
Reformado	29	5,6%
Não Respondeu	19	3,6%
Total	522	100%

Análise Quantitativa:

A grande maioria dos inquiridos está integrada no mercado de trabalho ou no sistema de ensino. 68% (61,5% + 6,5%) trabalham, sendo que 6,5% conciliam trabalho com estudo. Os estudantes representam 22,8% da amostra, enquanto os reformados são apenas 5,6%.

Interpretação Qualitativa:

Emergem um perfil de classe trabalhadora urbana, com altas taxas de ocupação e dupla jornada (estudo/trabalho). Isto desenha uma comunidade com rotinas intensas, possivelmente com menor tempo disponível para participação em iniciativas comunitárias ou de vigilância de bairro, facto que pode explicar parcialmente a baixa participação reportada em ações coletivas. A baixa taxa de reformados corrobora o caráter jovem da amostra e reflete a realidade demográfica e económica de bairros periféricos em contextos pós-conflito como o angolano.

Tabela 4 – Distribuição dos inquiridos por Tempo de Residência no Bairro

Tempo de Residência	Frequência (n)	Percentagem (%)
Mais de 10 anos	221	42,3%
4 a 6 anos	95	18,2%
7 a 10 anos	76	14,6%
1 a 3 anos	73	14,0%
Menos de 1 ano	42	8,0%
Não Respondeu	15	2,9%
Total	522	100%

Análise Quantitativa:

Observa-se um forte enraizamento local: 56,9% dos inquiridos (42,3% + 14,6%) residem no bairro há mais de 7 anos, e 42,3% há mais de uma década. Apenas 8% são residentes muito recentes (<1 ano).

Interpretação Qualitativa:

Esta estabilidade residencial indica laços comunitários sólidos e um conhecimento profundo da dinâmica do bairro. Tal enraizamento pode fomentar redes de apoio entre vizinhos e explicar por que 50,6% percebem uma cooperação positiva. No entanto, também pode criar "bolhas" sociais que dificultam a integração de novos moradores e perpetuar o desconhecimento de serviços externos de apoio (91,6% desconheciam serviços de apoio a vítimas). A baixa rotatividade sugere que as experiências de (in)segurança são partilhadas e acumuladas ao longo do tempo, influenciando fortemente a cultura local de segurança.

Tabela 5 – Distribuição dos inquiridos por Bairro de Residência

Bairro	Frequência (n)	Percentagem (%)
Pedalé	155	29,7%
Huambo	140	26,8%
Saber Andar	115	22,0%
Inorad	112	21,5%
Total	522	100%

Análise Quantitativa:

A amostra está distribuída de forma equilibrada entre quatro bairros, com nenhum a ultrapassar os 30% (Pedalé: 29,7%). Isto permite uma análise que captura a diversidade geográfica e potencialmente socioeconómica dentro da área de estudo.

Interpretação Qualitativa:

Esta diversidade é metodologicamente robusta, permitindo análises cruzadas e comparações entre bairros. Por exemplo, bairros com maior tempo de consolidação (como pode ser o caso dos com maior percentagem de residentes de longa data) podem apresentar diferentes dinâmicas de cooperação e percepção de crime em comparação com bairros em expansão. Pedalé, sendo o mais representado, pode ser um foco especial para entender vulnerabilidades específicas. Esta segmentação é crucial para políticas públicas que necessitem de intervenções micro-localizadas.

Tabela 6 – Distribuição dos inquiridos por Nível de Escolaridade

Escolaridade	Frequência (n)	Percentagem (%)
Secundário	231	44,3%
Superior	167	32,0%
Primário	85	16,3%
Nenhum	19	3,6%
Não Respondeu	20	3,8%
Total	522	100%

Análise Quantitativa:

O perfil educacional é relativamente elevado: 76,3% dos inquiridos (44,3% + 32,0%) possuem o ensino secundário ou superior. A taxa de analfabetismo formal (escolaridade "Nenhum") é baixa (3,6%).

Interpretação Qualitativa:

Este dado é relevante pois uma população com maior escolaridade tende a ter maior acesso a informação e, potencialmente, maior exigência perante as instituições. No entanto, a existência de um grupo significativo com apenas o ensino primário (16,3%) indica estratificação social. Qualitativamente, um nível educacional mais alto pode alimentar frustrações com a percebida ineficácia dos serviços policiais e contribuir para o ceticismo em relação à colaboração com as autoridades. Por outro lado, pode também ser um recurso para campanhas de prevenção e sensibilização mais sofisticadas.

2.2 Apresentação dos resultados das experiências de vitimização criminal

Tabela 7 – Experiência de Vitimização nos Últimos 12 Meses

Resposta	Frequência (n)	Percentagem (%)
Sim	292	55,9%
Não	230	44,1%
Total	522	100%

Análise Quantitativa:

Mais da metade dos inquiridos (55,9%) foi vítima de algum crime nos últimos 12 meses, indicando uma taxa de vitimização elevada que ultrapassa os 50%.

Interpretação Qualitativa:

Este dado evidência um contexto de insegurança significativa na comunidade. Comparando com médias internacionais (15-30% em inquéritos como o International Crime Victims Survey), a taxa de 55,9% é excepcionalmente alta, sugerindo fatores locais intensos como falhas na prevenção, insuficiência policial ou condições socioeconômicas que potenciam o risco criminal.

Tabela 8 – Tipos de Crime Reportados pelas Vítimas

Tipo de Crime	Contagem	Percentagem (%)
Roubo	203	69,5%
Furto	182	62,3%
Agressão	110	37,7%
Violência Doméstica	93	31,8%
Arrombamento	43	14,7%
Fraude	20	6,8%
Crime Cibernético	19	6,5%
Vandalismo	16	5,5%
Homicídio	13	4,5%
Extorsão	13	4,5%
Estupro	4	1,4%
Tráfico de Droga	2	0,7%
Sequestro	1	0,3%
Outro	5	1,7%

Análise Quantitativa:

Os crimes patrimoniais são os mais frequentes: roubo (69,5%) e furto (62,3%). Crimes contra a pessoa, como agressão (37,7%) e violência doméstica (31,8%), também têm incidência relevante. Crimes de alta gravidade (homicídio, estupro) apresentam percentagens baixas, mas são preocupantes.

Interpretação Qualitativa:

A predominância de roubos e furtos reflete um ambiente com falhas na vigilância e proteção de bens, coerente com a Teoria das Atividades Rotineiras. A presença significativa de violência interpessoal e doméstica aponta para a necessidade de políticas sociais e de prevenção de conflitos. O aparecimento de crimes cibernéticos (6,5%) indica a emergência de novas formas de criminalidade digital, exigindo adaptação das estratégias de segurança.

Tabela 9 – Número de Vezes que foi Vítima (Revitimização)

Nº de Vezes	Frequência (n)	Percentagem (%)
1	126	43,2%
2	79	27,1%
3	49	16,8%
4	26	8,9%
5 ou mais	12	4,1%
Total	292	100%

Análise Quantitativa:

Embora 43,2% tenham sido vítimas apenas uma vez, 56,8% sofreram vitimização múltipla (duas ou mais vezes). Destes, 4,1% foram vítimas cinco ou mais vezes.

Interpretação Qualitativa:

A alta taxa de revitimização sugere a existência de fatores de vulnerabilidade persistentes (como local de residência, rotinas ou perfil socioeconómico) que colocam certos indivíduos ou grupos em risco contínuo. Este fenómeno pode corroer a sensação de segurança e a confiança nas instituições, exigindo estratégias de prevenção direcionadas a essas "vítimas recorrentes".

Tabela 10 – Denúncia do Crime às Autoridades

Resposta	Frequência (n)	Percentagem (%)
Sim	91	31,2%
Não	201	68,8%
Total	292	100%

Análise Quantitativa:

Apenas 31,2% das vítimas denunciaram o crime. A maioria (68,8%) não o fez, indicando uma elevada "cifra negra" (crimes não reportados).

Interpretação Qualitativa:

Esta baixa taxa de denúncia reflete desconfiança nas autoridades, medo de represálias e percepção de ineficácia do sistema de justiça. Este padrão, comum em contextos onde a polícia é vista como distante ou ineficaz, constitui um obstáculo sério para o planeamento de políticas de segurança baseadas em dados reais.

Tabela 11 – Motivos para Não Denunciar

Motivo	Contagem	Percentagem (%)
Falta de confiança na polícia	125	62,2%
Sensação de inutilidade da denúncia	94	46,8%
Medo de represálias	70	34,8%
Dificuldade de acesso às autoridades	27	13,4%
Falta de provas ou testemunhas	23	211,4%
Envolvimento pessoal com o agressor	20	10,0%
Vergonha ou constrangimento	12	6,0%
Receio de ser culpabilizado(a)	9	4,5%
Desconhecimento sobre como denunciar	3	1,5%

Análise Quantitativa:

Os motivos principais são a falta de confiança na polícia (62,2%) e a sensação de que a denúncia não serviria para nada (46,8%). O medo de represálias (34,8%) também é significativo.

Interpretação Qualitativa:

Estes resultados confirmam uma crise de legitimidade e eficácia percebida das instituições policiais e judiciais. Para reduzir a cifra negra, é necessário reforçar a

proximidade policial-comunitária, garantir proteção às vítimas e comunicar eficazmente os resultados das investigações.

Tabela 12 – Horário de Ocorrência do Crime

Horário	Frequência (n)	Percentagem (%)
Noite	182	62,3%
Manhã	53	18,2%
Tarde	41	14,0%
Não Respondeu	16	5,5%
Total	292	100%

Análise Quantitativa:

A maioria esmagadora dos crimes ocorre durante a noite (62,3%), contrastando com os períodos diurnos (manhã: 18,2%; tarde: 14,0%).

Interpretação Qualitativa:

A noite é percecionada e confirmada como o período de maior vulnerabilidade, associado a menor movimentação, pior iluminação e possível intensificação de atividades criminosas. Isto aponta para a urgência de reforçar o policiamento noturno e melhorar a iluminação pública como medidas concretas de prevenção.

Tabela 13 – Número de Autores Envolvidos no Crime

Nº de Autores	Frequência (n)	Percentagem (%)
1	33	11,3%
2	125	42,8%
3 ou mais	119	40,8%
Não Respondeu	15	5,1%
Total	292	100%

Análise Quantitativa:

A criminalidade é predominantemente grupal: 83,6% dos crimes foram cometidos por dois ou mais autores.

Interpretação Qualitativa:

A prevalência de crimes em grupo (possivelmente assaltos ou ações coordenadas) aumenta o potencial de intimidação e violência, agravando o trauma das vítimas. Este padrão está alinhado com tendências internacionais e pode estar associado à atuação de gangues ou grupos criminosos locais, reforçando a perceção de insegurança organizada.

Tabela 14 – Danos e Consequências Sofridas pelas Vítimas

Tipo de Dano	Contagem	Percentagem (%)
Materiais	81	27,7%
Materiais + Psicológicos	67	22,9%
Físicos + Materiais + Psicológicos	40	13,7%
Materiais	39	13,4%
Físicos	21	7,2%
Psicológicos	19	6,5%
Físicos + Psicológicos	16	5,5%

Nota: Os inquiridos podiam assinalar mais de uma opção.

Análise Quantitativa:

Os danos materiais são os mais reportados (27,7% isoladamente, e presentes em várias combinações). Contudo, danos psicológicos e físicos também são significativos, especialmente em combinação com perdas materiais.

Interpretação Qualitativa:

Para além do prejuízo económico imediato, o crime produz impactos psicológicos e físicos duradouros que afetam o bem-estar e a qualidade de vida. A presença destes danos "invisíveis" sublinha a necessidade de serviços de apoio psicossocial às vítimas, que segundo os dados são largamente desconhecidos (91,6% não os conheciam).

2.3 Apresentação dos resultados da percepção de segurança

Tabela 15 – Identificação da Presença de Gangues ou Associações Criminosas

Resposta	Frequência (n)	Percentagem (%)
Sim	359	68,8%
Não	103	19,7%
Não sabe	46	8,8%
Não .Respondeu	14	2,7%
Total	522	100%

Análise Quantitativa:

Quase sete em cada dez inquiridos (68,8%) reconhecem a presença de gangues ou associações criminosas no bairro.

Interpretação Qualitativa:

Esta forte percepção associa diretamente a insegurança local à atuação de grupos organizados, possivelmente envolvidos em tráfico, assaltos em grupo ou conflitos territoriais. Esta perceção contribui para o medo do crime e pode minar a coesão social, além de pressionar por respostas de segurança que foquem no desmantelamento destas redes.

Tabela 16 – Sensação de Segurança ao Circular no Bairro

Período/ Sensação	Frequência (n)	Percentagem (%)
DIA		
Seguro(a)	222	42,5%
Nem seguro	103	19,7%
Nem inseguro(a)	93	17,8%
Muito seguro(a)	42	8,0%
Muito inseguro(a)	37	7,1%
Não Respondeu	25	4,8%

NOITE		
Inseguro/Muito Inseguro	≈ 245	≈ 46,9%
Seguro/Muito Seguro	≈ 124	≈ 23,8%

Nota: Os dados da noite são uma estimativa consolidada a partir da análise gráfica e textual.

Análise Quantitativa:

Durante o dia, a maioria sente-se segura (42,5%), mas apenas 8% se sentem muito seguros. À noite, a sensação inverte-se: quase metade sente-se insegura.

Interpretação Qualitativa:

Existe uma clara dicotomia dia/noite na percepção de segurança. O dia é associado a relativa normalidade, enquanto a noite é sinónimo de medo e restrição da mobilidade. Esta perceção está alinhada com os dados de ocorrência criminal (62,3% à noite) e reforça a necessidade de intervenções específicas para o período noturno.

Tabela 17 – Evolução da Sensação de Segurança (Comparação com Anos Anteriores)

Percepção da Evolução	Frequência (n)	Percentagem (%)
Melhorou	192	36,8%
Permaneceu igual	164	31,4%
Piorou	150	28,7%
Não Respondeu	16	3,1%
Total	522	100%

Análise Quantitativa:

As perceções estão divididas: 36,8% acham que melhorou, 31,4% que se manteve e 28,7% que piorou.

Interpretação Qualitativa:

Esta polarização reflete experiências heterogéneas na comunidade, possivelmente ligadas a diferenças entre bairros, grupos sociais ou exposição pessoal ao crime. Não há um consenso sobre uma trajetória clara de melhoria ou deterioração, o que sugere que as políticas de segurança têm impactos desiguais e precisam de ser mais segmentadas.

Tabela 18 – Factores que Contribuem para a Insegurança no Bairro

Factor	Contagem	Percentagem (%)
Ausência de policiamento frequente	364	69,7%
Falta de iluminação pública	362	69,3%
Desemprego/dificuldades económicas	239	45,8%
Áreas abandonadas ou degradadas	234	44,8%
Consumo e tráfico de drogas	161	30,8%
Falta de organização comunitária	125	23,9%
Conflitos entre grupos/gangues	125	23,9%
Falta de espaços de lazer para jovens	54	10,3%
Ineficiência da resposta policial	54	10,3%
Deficiências na infraestrutura urbana	19	3,6%
Violência física/sexual	18	3,4%
Violência doméstica	17	3,3%

Nota: Os inquiridos podiam assinalar mais de uma opção.

Análise Quantitativa:

Os dois factores mais citados são institucionais/estruturais: ausência de policiamento (69,7%) e falta de iluminação (69,3%). Factores socioeconómicos (desemprego: 45,8%) e urbanísticos (áreas degradadas: 44,8%) também são muito relevantes.

Interpretação Qualitativa:

A comunidade percebe a insegurança como um problema multidimensional, resultante da falta do Estado (policiamento, iluminação, infraestrutura) e de fragilidades sociais e urbanas. A solução exigirá uma abordagem integrada que combine reforço policial, investimento urbano, políticas sociais e envolvimento comunitário.

Tabela 19 – Medidas de Protecção Adoptadas pelos Residentes

Medida	Contagem	Percentagem (%)
Evitar sair à noite	358	68,6%
Evitar andar sozinho(a) em certas áreas	228	43,7%
Reforçar fechaduras/instalar alarmes	215	41,2%
Mudar rotina ou trajeto diário	113	21,6%
Não adoptou nenhuma medida	55	10,5%
Carregar item de defesa pessoal	46	8,8%
Pedir apoio a amigos/família	36	6,9%
Participar em vigilância comunitária	27	5,2%
Contratar segurança privada	5	1,0%

Nota: Os inquiridos podiam assinalar mais de uma opção.

Análise Quantitativa:

As medidas mais comuns são comportamentais e preventivas: evitar sair à noite (68,6%), evitar áreas (43,7%) e reforçar a segurança da casa (41,2%). Medidas colectivas (vigilância comunitária: 5,2%) ou proactivas (defesa pessoal: 8,8%) são menos frequentes.

Interpretação Qualitativa:

A resposta predominante à insegurança é a "autoprotecção pela evitação", o que reflecte uma adaptação individual ao risco e uma certa descrença na capacidade colectiva ou institucional de protecção. Este comportamento tem custos sociais, restringindo a liberdade de circulação e a vida comunitária, especialmente à noite.

2.4 Síntese geral e conclusões interpretativas

A análise dos dados de vitimização e percepção de segurança revela um quadro complexo e preocupante no município da Samba:

1. Alta Vitimização e Revitimização: Com 55,9% de vítimas no último ano e 56,8% de vitimização múltipla, a comunidade vive uma exposição crónica ao crime, especialmente a roubos e furtos.

2. Crise de Confiança Institucional: Apenas 31,2% das vítimas denunciam, principalmente devido à desconfiança na polícia e à percepção de inutilidade do acto. Esta cifra negra elevada dificulta o diagnóstico e o combate eficaz ao crime.

3. Insegurança Noturna e Percepção de Criminalidade Organizada: A noite é o período de maior risco (62,3% dos crimes) e de maior medo. A forte percepção da presença de gangues (68,8%) alimenta o sentimento de vulnerabilidade.

4. Percepção Multifatorial da Insegurança: A população atribui a insegurança a falhas institucionais (policiamento, iluminação) e a problemas estruturais (desemprego, degradação urbana), exigindo respostas integradas.

5. Estratégias de Coping Centradas na Evitação: A resposta individual mais comum é restringir a mobilidade (especialmente noturna), o que reflecte uma adaptação defensiva ao meio e um recuo da vida pública em horários considerados perigosos.

Podemos observer que os dados desenham uma comunidade jovem, enraizada e activa, mas que enfrenta níveis elevados de criminalidade patrimonial e violência interpessoal, com uma perceção de insegurança agravada pela noite e pela desconfiança nas instituições. A solução passa necessariamente por reforçar a presença e legitimidade policial, melhorar as condições urbanas (iluminação, espaços), combater as causas socioeconómicas do crime e fomentar uma maior organização e participação comunitária em estratégias de prevenção e apoio às vítimas.

2.1.4 Síntese geral e conclusões interpretativas

A análise dos dados revela um quadro complexo e preocupante no município da Samba. Com 55,9% de vítimas no último ano e 56,8% de vitimização múltipla, a comunidade vive uma exposição crónica ao crime, especialmente a roubos e furtos. Apenas 31,2% das vítimas denunciam, principalmente devido à desconfiança na polícia e à percepção de inutilidade, o que configura uma cifra negra elevada. A noite é o período de maior risco (62,3% dos crimes) e de maior medo, e 68,8% identificam a presença de gangues. A população atribui a insegurança a falhas institucionais (policiamento, iluminação) e a problemas estruturais (desemprego, degradação urbana). A resposta individual mais comum é restringir a mobilidade nocturna.

Estes dados constituem o insumo de domínio que alimenta a plataforma digital apresentada na secção seguinte, validando a sua necessidade e fundamentando as funcionalidades de análise estatística, denúncia e consulta inteligente de dados.

2.2 Concepção, construção e validação da plataforma digital

Nesta secção, é apresentada a plataforma digital Vitmização Angola, descrevendo a sua arquitectura, funcionalidades e principais componentes técnicos. A plataforma foi concebida como um sistema de informação web que integra funcionalidades de recolha, armazenamento, processamento estatístico, geração de relatórios e interacção inteligente com o utilizador, adoptando a metodologia ágil Extreme Programming (XP) como modelo de processo de desenvolvimento.

O código-fonte completo encontra-se disponível no repositório público: https://github.com/edconsultingangola/indice-criminalidade

2.2.1 Aplicação da metodologia Extreme Programming

O desenvolvimento seguiu os ciclos iterativos da XP, conforme evidenciado pela evolução das migrações da base de dados (Prisma): a primeira migração (init, Novembro 2025) criou o esquema base com as entidades Resident, Victimization e SecurityPerception; migrações subsequentes adicionaram o modelo User (autenticação), reestruturaram campos de arrays para campos booleanos individuais (compatibilidade SQLite), e introduziram o modelo Report (denúncias, Janeiro 2026). Este padrão de evolução incremental é consistente com os princípios da XP de design simples e refactoring contínuo.

A metodologia aplicada caracterizou-se pela comunicação constante entre a equipa de desenvolvimento e os utilizadores-alvo, pela simplicidade das soluções implementadas em cada iteração, pelo feedback rápido através de entregas frequentes de módulos funcionais, e pela coragem para alterar decisões de design quando os testes o exigiram.

2.2.2 Arquitectura do sistema

A plataforma SafeAngola é uma aplicação web full-stack com arquitectura separada em camadas, construída sobre o ecossistema JavaScript/TypeScript:

Camada	Tecnologias	Função
Front-end	React 18, Next.js 14, TypeScript, Tailwind CSS, shadcn-ui, Radix UI, Recharts	Interface, dashboards interactivos, formulários, chatbot
Back-end	Next.js API Routes, Node.js, Prisma ORM, bcryptjs, nodemailer, Zod	Lógica de negócio, autenticação, APIs RESTful
Base de dados	SQLite via Prisma ORM (6 migrações)	Persistência com integridade referencial
Motor Pericial	Python 3, Flask, Pandas, NumPy, Google Gemini AI	Pré-processamento, análise pericial, IA
Infraestrutura	Docker, docker-compose	Containerização e portabilidade

A análise do repositório revela uma base de código com 10.800 linhas de código TypeScript/TSX distribuídas por 17 páginas de dashboard, 22 rotas de API e 15 componentes de aplicação (além de 48 componentes de UI reutilizáveis). O motor pericial Python conta com 2.125 linhas adicionais.

2.2.3 Modelo de dados

O esquema da base de dados (schema.prisma) reflecte directamente a estrutura do inquérito de vitimização criminal, demonstrando a articulação entre a investigação criminológica e a engenharia de software:

Entidade	Campos	Correspondência no Inquérito
Resident	~30	Secção I — Dados Sociodemográficos (idade, género, ocupação, bairro, escolaridade, medidas de protecção)
Victimization	~35	Secção II — Experiências de Vitimização (tipo de crime, frequência, denúncia, motivos, horário, autores, danos) + Secção III (gangues)
SecurityPerception	~28	Secção IV — Percepção de Segurança (dia/noite, evolução, factores, confiança policial)
Report	~18	Módulo de denúncias — dados do denunciante, tipo de crime, estado da ocorrência
User	7	Gestão de utilizadores — autenticação, perfis (ADMIN, RESEARCHER, POLICE, CITIZEN)

A opção por campos booleanos individuais (13 campos para tipos de crime, 10 para motivos de não denúncia, 13 para factores de insegurança) em vez de arrays justifica-se pela limitação do SQLite, conforme evidenciado na migração update_schema_for_sqlite_arrays.

2.2.4 Funcionalidades principais

a) Autenticação e gestão de utilizadores

O sistema implementa autenticação por email/senha com hashing bcrypt, suportando quatro perfis: ADMIN (gestão completa), RESEARCHER (análise e relatórios), POLICE (gestão de ocorrências) e CITIZEN (denúncias e consultas). A recuperação de senha é realizada via link seguro enviado por email através do nodemailer.

b) Importação de dados Excel

A funcionalidade de importação (283 linhas de código) permite carregar ficheiros Excel (.xlsx) com os dados dos inquéritos. O sistema valida a estrutura do ficheiro (colunas esperadas), realiza a importação de forma transacional (com rollback em caso de erro) e apresenta relatório detalhado com contagem de registos e erros.

c) Dashboards e análise estatística

A plataforma disponibiliza 12 endpoints de análise estatística dedicados, cada um com visualização gráfica interactiva via Recharts: distribuição de crimes por bairro, vitimização cruzada por faixa etária e género, frequência por tipo de crime, motivos de subnotificação, percepção de segurança dia vs. noite, nível de confiança na polícia, percepção por género, correlação entre percepção e presença policial, vitimização por ocupação e por nível de escolaridade, distribuição demográfica e indicadores-chave consolidados.

d) Sistema de denúncias

O módulo de denúncias permite que cidadãos registem ocorrências de forma pública ou anónima, com campos para tipo de crime, descrição, localização e dados sociodemográficos opcionais. O sistema envia confirmação por email, gera notificação interna (com polling de 30 segundos) e permite à polícia acompanhar e actualizar o estado das ocorrências (Pendente, Em Análise, Encaminhado, Resolvido).

e) Chatbot inteligente (Motor Pericial)

O chatbot constitui o principal diferencial tecnológico da plataforma. A sua arquitectura divide-se em quatro camadas:

Pré-processamento (PreProcessadorCriminal): classe Python com método de classe que limpa, organiza e enriquece os dados dos inquéritos, criando variáveis derivadas como índice de risco por bairro, categoria de risco e scores de severidade.

Motor Pericial (MotorPericial): núcleo científico com 5 módulos de análise — perfil de vitimização, análise de denúncia, análise de percepção de segurança, análise institucional e análise causal-social — aplicando correlação de Pearson, teste Qui-Quadrado, ANOVA e teste t-Student.

Integração com IA (Google Gemini): o sistema gera um contexto estatístico completo e envia-o ao modelo gemini-2.5-flash para gerar respostas em linguagem natural. A IA responde exclusivamente com base nos dados fornecidos, garantindo rigor científico.

API RESTful com autenticação por token: o motor pericial expõe endpoints (/api/v1/query, /api/v1/stats, /api/v1/query-chart) protegidos por tokens de API, permitindo integração com o front-end e sistemas externos.

f) Geração de relatórios e exportação

A plataforma permite gerar relatórios analíticos com exportação em múltiplos formatos (PDF, Excel, imagem), com filtros aplicados e metadados.

g) Funcionalidades complementares

O sistema inclui ainda: tema claro/escuro via next-themes; módulo de backup e restauração da base de dados; logs e auditoria de acções críticas; e página de serviços de apoio às vítimas.

2.2 Requisitos funcionais (RF)

São descrições das funcionalidades que o sistema deve oferecer para satisfazer as necessidades dos utilizadores.

Tabela 2.

Requisitos funcionais

Nº	Tipo	Requisito	Descrição
RF01	Funcional	Cadastro de usuário	Permite registro de usuários (ADMIN, RESEARCHER, POLICE, CITIZEN) via e-mail e senha; valida e-mail único; senha armazenada com hash; sessões protegidas.
RF02	Funcional	Login por perfil	Permite login por e-mail/senha com perfis diferenciados; rotas e componentes protegidos por papel; UI mostra apenas opções autorizadas.
RF03	Funcional	Recuperação de senha	Permite recuperação de senha via link seguro enviado por e-mail.
RF04	Funcional	Gestão de perfil	Usuários podem editar nome, e-mail, foto e avatar; alterações persistem e são exibidas no perfil.
RF05	Funcional	Envio de denúncias	Permite envio de denúncias públicas ou anônimas (tipo de crime, descrição, localização); denúncia salva, e-mail enviado/confirmado.
RF06	Funcional	Gestão de ocorrências	Administradores e investigadores podem listar, filtrar, ordenar e marcar ocorrências como lidas ou analisadas; contador de notificações atualizado.
RF07	Funcional	Notificações	Indicador de novas denúncias com polling periódico (ex.: 30s); contador reflete alterações; clique redireciona para ocorrências.
RF08	Funcional	Importação de dados Excel	Permite upload de arquivos .xlsx/.xls; valida colunas (ex: 103 colunas); erros detalhados; dados válidos importados; transação segura (rollback em falha).

RF09	Funcional	Gráficos e análises	Dashboards com gráficos interativos (faixa etária, tipos de crime, bairros, percepção de segurança); exportação para PDF/Excel/Imagem.
RF10	Funcional	Chatbot inteligente	Interface para consultas em linguagem natural sobre os dados; gera sumários e relatórios; apresenta fonte/dados usados.
RF11	Funcional	Relatórios técnicos	Criação, visualização e exportação de relatórios em PDF/Excel com base em dados de inquéritos de vitimização.
RF12	Funcional	Gestão de usuários	Administradores podem criar, editar, desativar usuários; atribuir papéis; histórico de alterações persistente.
RF13	Funcional	Persistência e infraestrutura	Uso de Prisma com SQLite; suporte a migrations; geração de client; compatível com Prisma Studio; backup/restauração.
RF14	Funcional	Logs e auditoria	Registro de eventos críticos (login, importações, alterações, validações falhadas); administrador pode listar eventos com timestamp e usuário executor.
RF15	Funcional	Tratamento de erros	Mensagens amigáveis ao usuário; logs detalhados para desenvolvedor; evita exposição de stack trace; possibilita debugging.
RF16	Funcional	Filtros e consultas	Permite filtrar ocorrências e inquéritos por tipo de crime, bairro, idade, gênero, e outros critérios múltiplos.
RF17	Funcional	Tema claro/escuro	Permite alternar entre modo claro e escuro em todas as páginas da plataforma para melhor experiência de usuário.

Fonte: Elaborado pela autora, 2026

2.3 Requisitos não funcionais (RNF)

Correspondem às características de qualidade, desempenho e restrições que o sistema deve atender. Esses requisitos não descrevem funções específicas do sistema, mas definem como o sistema deve operar, incluindo aspectos como segurança, usabilidade, desempenho e confiabilidade.

Tabela 3.

Requisitos não funcionais

Nº	Tipo	Requisito	Descrição
RNF01	Não Funcional	Performance	UI deve responder em < 500 ms para 95% das requisições; teste de carga confirma percentil ≤ 500 ms em dashboards.
RNF02	Não Funcional	Escalabilidade	Arquitetura preparada para escalar horizontalmente; aplicação suporta adicionar réplicas via Docker/orquestrador sem alterar código.
RNF03	Não Funcional	Disponibilidade	Disponibilidade alvo de 99,5% em produção; métricas de uptime confirmam SLA mensal.
RNF04	Não Funcional	Confiabilidade / Tolerância a Falhas	Operações críticas (importação Excel, gravação denúncias) com retry e rollback; falhas provocam rollback e registro de erro.
RNF05	Não Funcional	Segurança	TLS obrigatório; senhas com hash (bcrypt); proteção contra CSRF, XSS e SQL Injection; testes de penetração não encontram vulnerabilidades críticas.
RNF06	Não Funcional	Privacidade / Proteção de Dados	Dados pessoais minimizados; logs não contêm PII; conformidade com legislação local (GDPR-like); políticas de

			retenção definidas e anonimização possível.
RNF07	Não Funcional	Criptografia	Dados em trânsito via HTTPS; backups e credenciais armazenados criptografados; arquivos sensíveis não em texto plano.
RNF08	Não Funcional	Backup e Recuperação	Backups regulares; restauração testada; recuperação em ambiente de teste < 1 hora.
RNF09	Não Funcional	Manutenibilidade	Código modular, documentação mínima, scripts npm para tarefas comuns; novo dev consegue rodar projeto local em ≤ 30 minutos.
RNF10	Não Funcional	Extensibilidade	Interfaces e serviços desacoplados; novas integrações (NLP/LLM, fontes de dados) adicionáveis sem refatoração extensa.
RNF11	Não Funcional	Usabilidade	Interface intuitiva, fluxo claro para importação e denúncia; mensagens de erro amigáveis; teste com usuários não técnicos completando tarefas críticas.
RNF12	Não Funcional	Acessibilidade	Segue WCAG básico (contraste, navegação por teclado, labels em formulários); ferramentas automáticas confirmam ausência de erros críticos.
RNF13	Não Funcional	Compatibilidade / Portabilidade	Suporte a navegadores modernos (Chrome, Firefox, Edge, Safari) e responsividade mobile; páginas renderizam corretamente em dispositivos móveis e desktop.

RNF14	Não Funcional	Observabilidade (Logs & Monitoramento)	Logs estruturados; métricas básicas (requests, erros, tempo médio); alertas configurados para erros críticos; dashboards exibem métricas.
RNF15	Não Funcional	Testabilidade e Qualidade	Suite mínima de testes unitários e E2E; integração contínua; CI executa lint + testes; cobertura mínima documentada.
RNF16	Não Funcional	Tempo de Recuperação e Continuidade	RTO ≤ 2 horas para incidentes críticos; RPO ≤ 24 horas; procedimentos documentados e testados.
RNF17	Não Funcional	Conformidade Legal e Retenção	Políticas de retenção, consentimento quando necessário e registro de auditoria; flags e timestamps implementados.
RNF18	Não Funcional	Implantação e Automação	Suporte a containerização (Docker); scripts de build/deploy; build reproducível com npm run build; projeto roda via docker-compose.

Fonte: Elaborado pela autora, 2026

2.4 Casos de uso

A modelação de casos de uso permite representar as funcionalidades do sistema e as interações entre os utilizadores (actores) e a plataforma digital. O diagrama de casos de uso descreve de forma clara como os diferentes actores interagem com o sistema de recolha, gestão e análise de dados de vitimização criminal.

Tabela 4.

Casos de uso

Código	Nome do caso de uso	Ator(es)	Descrição
UC01	Registar conta	Cidadão, Investigador, Polícia	Permite que novos usuários criem uma conta na plataforma; valida e-mail único e armazena senha com hash; sessão iniciada após registro.
UC02	Efetuar login	Cidadão, Investigador, Polícia, Administrador	Permite acesso ao sistema via email/senha; sessões seguras; bloqueio de acesso em caso de permissão insuficiente.
UC03	Recuperar senha	Todos os utilizadores	Permite redefinir a senha via link enviado por email; link expira após período definido; senha armazenada com hash.
UC04	Editar perfil	Todos os utilizadores	Permite atualizar nome, email e avatar; alterações persistem no banco e refletem imediatamente na UI; valida email duplicado.
UC05	Enviar denúncia	Cidadão	Permite registrar denúncias públicas ou anônimas (assunto, descrição, localização); sistema valida, salva e envia confirmação por email; gera notificação interna.
UC06	Consultar denúncia	Cidadão, Polícia	Permite consultar o estado de uma denúncia registrada; exibe informações atualizadas sobre análise ou resolução.
UC07	Atualizar estado da denúncia	Polícia	Permite atualizar status da ocorrência (em análise, resolvido, etc.); sistema persiste alterações e atualiza

			contadores/notificações; acesso restrito por perfil.
UC08	Visualizar ocorrências	Polícia, Administrador	Permite listar, filtrar e ordenar todas as ocorrências registradas; acesso restrito por perfil; alterações de status refletidas em tempo real.
UC09	Importar dados Excel	Administrador	Permite upload de arquivos Excel com validação de colunas e estrutura; importação transacional com rollback em caso de erro; relatório de importação apresentado.
UC10	Visualizar gráficos estatísticos	Investigador, Administrador	Permite visualizar dashboards interativos com filtros (faixa etária, tipo de crime, bairros); exportação para PDF/Excel/Imagem disponível.
UC11	Gerar relatórios	Investigador	Permite criar relatórios analíticos em PDF a partir de dados importados ou registrados; inclui filtros aplicados e metadados.
UC12	Exportar dados	Investigador, Administrador	Permite exportar dados em formatos Excel, CSV ou PDF; mantém filtros e metadados; tratamento de erros e retry em caso de falha.
UC13	Gerir utilizadores	Administrador	Permite criar, editar ou remover usuários; atribuir papéis; ações registradas em auditoria; alterações refletidas imediatamente.
UC14	Realizar backup	Administrador	Permite criar cópias de segurança da base de dados; backups regulares e armazenados com criptografia.

UC15	Restaurar backup	Administrador	Permite restaurar dados a partir de backup; valida integridade dos dados; RTO ≤ 2 horas.
UC16	Receber notificações	Todos os utilizadores	Sistema envia alertas sobre novas denúncias, atualizações de ocorrências ou eventos importantes; contador atualizado via polling.
UC17	Procurar serviços de apoio	Cidadão	Permite encontrar instituições e serviços de apoio às vítimas de crimes; informações filtráveis por localização ou tipo de serviço.
UC18	Visualizar estatísticas de vitimização	Investigador	Permite analisar padrões de criminalidade, frequências e áreas de risco; gráficos e dashboards interativos.
UC19	Utilizar chatbot inteligente	Cidadão, Investigador	Permite interagir com chatbot para consultas em linguagem natural; respostas baseadas em dados de vitimização; fallback em caso de falha de integração.
UC20	Alternar tema do sistema	Todos os utilizadores	Permite mudar tema da interface entre claro e escuro; alterações refletidas imediatamente em todas as páginas.

Fonte: Elaborado pela autora, 2026

2.4.1 Descrição dos casos de uso

Actores do Sistema

Atores Primários

Cidadão

- Utilizador que pode reportar situações de vitimização criminal, consultar o estado de denúncias, interagir com o chatbot inteligente, procurar serviços de apoio e personalizar sua experiência na plataforma (ex.: alternar tema).

Investigador

- Responsável pela análise científica dos dados recolhidos, geração de relatórios estatísticos, visualização de dashboards, criação de gráficos e exportação de dados.

Polícia

- Responsável por acompanhar denúncias, verificar ocorrências, atualizar o estado das investigações, gerir notificações de incidentes e marcar ocorrências como lidas ou resolvidas.

Administrador

- Responsável pela gestão completa da plataforma, incluindo criação, edição e remoção de usuários, atribuição de papéis, auditoria de ações, manutenção da base de dados e realização de backups e restaurações.

Actores Secundários

Sistema de Email

- Responsável pelo envio automático de notificações, confirmações de denúncias, links de redefinição de senha e alertas de atualização do sistema.

Base de Dados

- Armazena todas as informações do sistema, incluindo usuários, denúncias, ocorrências, dados importados (Excel) e registros de auditoria.

Sistema de Ficheiros

- Responsável pelo armazenamento seguro de documentos e ficheiros importados, como planilhas Excel utilizadas para análise de vitimização.

UC01 – Registar conta

- **Atores:** Cidadão, Investigador, Polícia
- **Objetivo:** Permitir que novos utilizadores criem uma conta na plataforma; valida e-mail único e armazena senha com hash; sessão iniciada após registro.
- **Pré-condições:** O utilizador deve possuir acesso à internet e Deve possuir um endereço de email válido.
- **Fluxo principal:**

1. O utilizador acede à página de registo.
2. Preenche o formulário com os seus dados pessoais.
3. Define email e senha.
4. Submete o formulário.

5. O sistema valida os dados.
6. A conta é criada na plataforma e a sessão é iniciada.

- Fluxo alternativo:
- Email já existente → o sistema informa erro.
- Dados incompletos → sistema solicita correção antes da submissão.
  Pós-condições: O utilizador possui uma conta ativa no sistema.

UC02 – Efetuar login

Atores: Cidadão, Investigador, Polícia, Administrador
Objetivo: Permitir acesso ao sistema via email/senha; sessões seguras; bloqueio de acesso em caso de permissão insuficiente.
Pré-condições: O utilizador deve possuir conta cadastrada.
Fluxo principal:

1. O utilizador acede à página de login.
2. Introduz email e senha.
3. O sistema valida as credenciais.
4. O sistema redireciona para o painel correspondente ao perfil do usuário.
   Fluxo alternativo: Senha incorreta → sistema sugere recuperar senha.
   Pós-condições: O utilizador fica autenticado no sistema.

UC03 – Recuperar senha

Atores: Todos os utilizadores
Objetivo: Permitir redefinição de senha via link enviado por email; link expira após período definido; senha armazenada com hash.
Pré-condições: O utilizador deve possuir conta no sistema.
Fluxo principal:

1. Seleciona “Esqueci minha senha”.
2. Introduz o email associado à conta.
3. O sistema verifica a existência do email.
4. Envia link de recuperação.
5. O utilizador redefine a senha.
   Fluxo alternativo: Email não encontrado → sistema apresenta aviso.
   Pós-condições: Senha atualizada.

UC04 – Editar perfil

Atores: Todos os utilizadores
Objetivo: Permitir atualizar nome, email e avatar; alterações persistem no banco e

refletem imediatamente na UI; valida email duplicado.
Pré-condições: O utilizador deve estar autenticado.
Fluxo principal:

1. Acede à área de perfil.
2. Edita informações pessoais.
3. Submete alterações.
4. Sistema atualiza os dados no banco e na UI.
   Fluxo alternativo: Email em uso → erro exibido.
   Pós-condições: Perfil atualizado no sistema.

UC05 – Enviar denúncia

Ator: Cidadão
Objetivo: Permitir registrar denúncias públicas ou anônimas; sistema valida, salva e envia confirmação por email; gera notificação interna.
Pré-condições: O cidadão deve estar autenticado.
Fluxo principal:

1. Acede à área de denúncia.
2. Preenche assunto, descrição, tipo de crime, local e data.
3. (Opcional) Anexa documentos.
4. Submete denúncia.
5. Sistema valida e registra ocorrência.
6. Envia confirmação por email e cria notificação interna.
   Fluxo alternativo: Informação obrigatória faltando → sistema solicita preenchimento.
   Pós-condições: Denúncia registrada na base de dados.

UC06 – Consultar denúncia

Atores: Cidadão, Polícia
Objetivo: Permitir consultar o estado de uma denúncia registrada; exibe informações atualizadas sobre análise ou resolução.
Pré-condições: Deve existir uma denúncia registrada.
Fluxo principal:

1. Acede à área de consulta.
2. Introduz número da denúncia ou aplica filtros.
3. Sistema apresenta detalhes da ocorrência.
   Pós-condições: Estado da denúncia visualizado.

UC07 – Atualizar estado da denúncia

Ator: Polícia
Objetivo: Permitir atualizar status da ocorrência (em análise, resolvido, etc.); alterações persistidas e notificações atualizadas; acesso restrito por perfil.
Pré-condições: Denúncia existente no sistema.
Fluxo principal:

1. Acessa lista de ocorrências.
2. Seleciona uma denúncia.
3. Atualiza estado.
4. Sistema persiste alteração e atualiza contadores/notificações.
   Pós-condições: Estado da denúncia atualizado.

UC08 – Visualizar ocorrências

Atores: Polícia, Administrador
Objetivo: Listar, filtrar e ordenar ocorrências registradas; alterações refletidas em tempo real.
Pré-condições: Usuário autenticado.
Fluxo principal:

1. Acessa painel de ocorrências.
2. Sistema apresenta lista de ocorrências.
3. Aplica filtros e ordenações.
   Pós-condições: Ocorrências visualizadas corretamente.

UC09 – Importar dados Excel

Ator: Administrador
Objetivo: Importar dados de vitimização a partir de ficheiros Excel; validação de colunas/estrutura; transação com rollback em caso de erro.
Pré-condições: Administrador autenticado.
Fluxo principal:

1. Acessa área de importação.
2. Seleciona ficheiro Excel.
3. Sistema valida e importa dados.
   Fluxo alternativo: Ficheiro inválido → apresenta erro e aborta operação.
   Pós-condições: Dados disponíveis no sistema.

UC10 – Visualizar gráficos estatísticos

Atores: Investigador, Administrador
Objetivo: Visualizar dashboards interativos com filtros; exportação para PDF/Excel/Imagem.
Pré-condições: Dados existentes na base.
Fluxo principal:

1. Acessa área de estatísticas.
2. Seleciona tipo de análise e filtros.
3. Sistema gera gráficos interativos.
   Pós-condições: Estatísticas apresentadas; opção de exportação disponível.

UC11 – Gerar relatórios

Ator: Investigador
Objetivo: Criar relatórios analíticos em PDF com base em dados importados ou registrados; inclui filtros e metadados.
Fluxo principal:

1. Seleciona tipo de relatório.
2. Sistema processa os dados.
3. Relatório gerado em PDF.

UC12 – Exportar dados

Atores: Investigador, Administrador
Objetivo: Exportar dados em Excel, CSV ou PDF; mantém filtros e metadados; retry em caso de falha.
Fluxo principal:

1. Seleciona dados e formato.
2. Sistema gera arquivo para download.

UC13 – Gerir utilizadores

Ator: Administrador
Objetivo: Criar, editar ou remover usuários; atribuir papéis; ações registradas em auditoria; alterações imediatas.
Fluxo principal:

1. Acessa área de gestão de usuários.
2. Cria, edita ou remove usuários.

3. Sistema registra auditoria.

UC14 – Realizar backup

Ator: Administrador
Objetivo: Criar cópias de segurança da base de dados com criptografia.
Fluxo principal:

1. Seleciona opção de backup.
2. Sistema gera cópia da base de dados.
3. Arquivo armazenado com segurança.

UC15 – Restaurar backup

Ator: Administrador
Objetivo: Restaurar dados da base a partir de backup; valida integridade; RTO ≤ 2h.
Fluxo principal:

1. Seleciona arquivo de backup.
2. Sistema valida e restaura dados.

UC16 – Receber notificações

Ator: Sistema (automático)
Objetivo: Informar utilizadores sobre novas denúncias, atualizações de ocorrências ou eventos importantes.
Fluxo principal:

1. Sistema detecta evento relevante.
2. Gera e envia notificação ao utilizador.

UC17 – Procurar serviços de apoio

Ator: Cidadão
Objetivo: Localizar instituições e serviços de apoio às vítimas.
Fluxo principal:

1. Acede à área de serviços de apoio.
2. Introduz filtros ou localização.
3. Sistema apresenta resultados disponíveis.

UC18 – Visualizar estatísticas de vitimização

Ator: Investigador
Objetivo: Analisar padrões de criminalidade, frequências e áreas de risco; dashboards interativos.
Fluxo principal:

1. Seleciona variáveis de análise.
2. Sistema processa dados.
3. Resultados apresentados em gráficos e indicadores.

UC19 – Utilizar chatbot inteligente

Atores: Cidadão, Investigador
Objetivo: Interagir com chatbot para consultas em linguagem natural; respostas baseadas em dados de vitimização; fallback em caso de falha.
Pré-condições: Base de dados carregada.
Fluxo principal:

1. Abre chatbot.
2. Introduz pergunta.
3. Sistema processa pergunta.
4. Consulta base de dados.
5. Gera resposta baseada nos dados.
6. Apresenta resposta ao utilizador.

UC20 – Alternar tema do sistema

Atores: Todos os utilizadores
Objetivo: Alterar o tema da interface (claro/escuro).
Fluxo principal:

1. Acede às configurações.
2. Seleciona tema desejado.
3. Sistema aplica tema em todas as páginas.
   Pós-condições: Interface atualizada com o tema escolhido.

2.5 Diagrama de Caso de Uso

este diagrama representa as principais funcionalidades do sistema de análise de vitimização criminal, destacando os diferentes actores envolvidos, como o **cidadão, polícia, investigador e administrador**, bem como a própria plataforma.

O diagrama apresenta os principais casos de uso do sistema, tais como registo de utilizadores, autenticação (login), envio e consulta de denúncias, visualização de ocorrências, importação de dados em ficheiros Excel, geração de relatórios estatísticos, exportação de dados, gestão de utilizadores e utilização do chatbot inteligente para consulta de informações relacionadas com a vitimização.

Além disso, o diagrama também inclui os relacionamentos include e extend, que demonstram dependências entre funcionalidades e possíveis fluxos alternativos dentro do sistema. Estes relacionamentos permitem compreender como determinadas funcionalidades dependem de outras para serem executadas ou podem ser activadas como extensões de um processo principal.

Desta forma, o diagrama de caso de uso facilita a compreensão das interações entre os utilizadores e o sistema, contribuindo para a análise dos requisitos e para o desenvolvimento da plataforma digital de recolha, gestão e análise de dados de vitimização criminal.

Figura 22.
Diagrama de Caso de Uso.

Fonte: Elaborado pelo autor, 2026.

.2.6 Diagrama de Classe

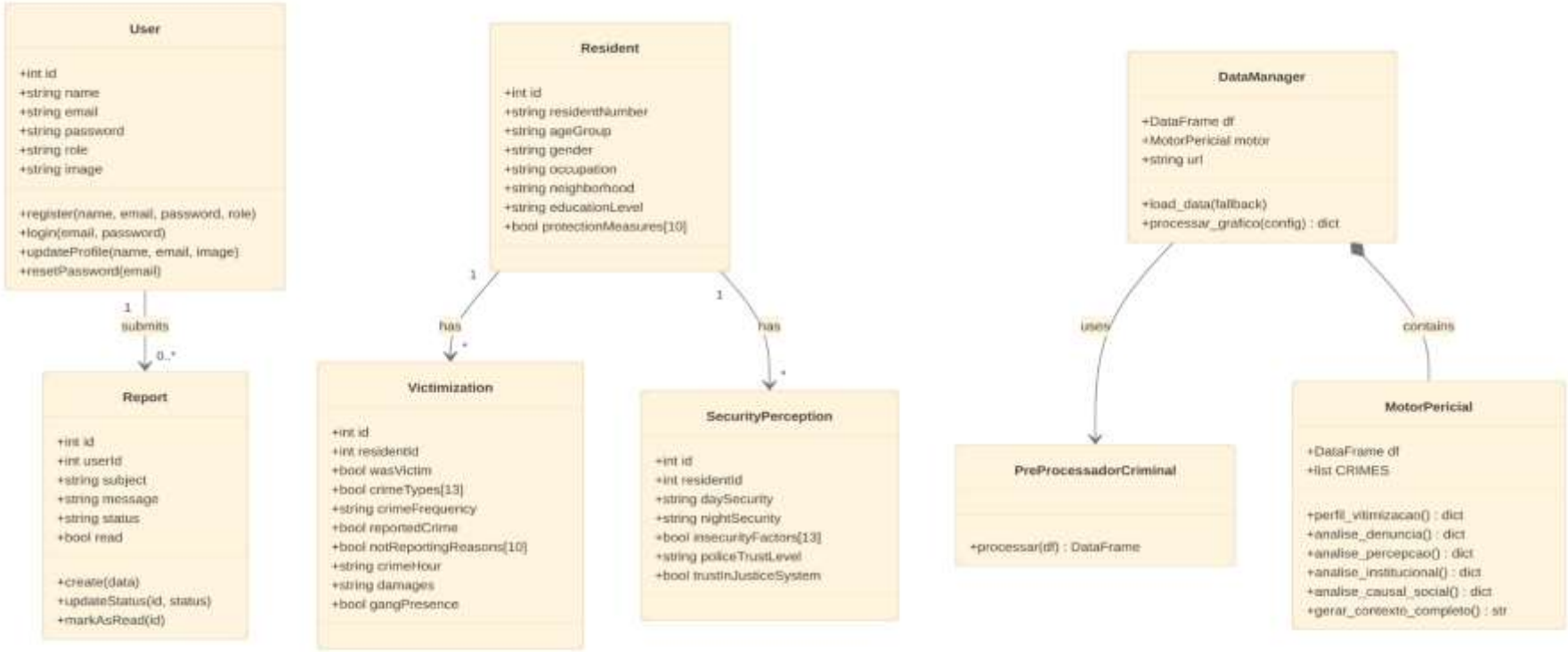
este diagrama representa a estrutura lógica do sistema de análise de vitimização criminal, mostrando as principais classes que compõem a plataforma, tais como Utilizador, Cidadão, Polícia, Investigador, Administrador, Denúncia, Dados de Vitimização, Relatórios, Estatísticas, Chatbot e Notificações, juntamente com os seus respectivos atributos e métodos.

O diagrama evidencia também os relacionamentos existentes entre as classes. Por exemplo, um utilizador pode assumir diferentes perfis dentro do sistema, como cidadão, polícia, investigador ou administrador. O cidadão pode registar denúncias de vitimização, enquanto a polícia pode consultar e actualizar o estado dessas ocorrências. Os investigadores têm acesso aos dados de vitimização para análise estatística e geração de relatórios, permitindo compreender padrões de criminalidade e vitimização.

Além disso, as denúncias estão associadas aos dados registados na base de dados e podem gerar notificações automáticas enviadas aos utilizadores do sistema. O chatbot inteligente também se encontra ligado aos dados de vitimização armazenados, permitindo responder a perguntas feitas pelos utilizadores com base nas informações existentes na base de dados.

Desta forma, o diagrama de classe demonstra como os diferentes componentes da plataforma estão organizados e interligados, contribuindo para a estruturação da arquitectura orientada a objectos do sistema.

Figura 23.
Diagrama de Classe.



Fonte: Elaborado pelo autor, 2026.

2.7 Diagrama Entidade-Relacionamento (ER)

este diagrama descreve a organização física dos dados no banco de dados do sistema de análise de vitimização criminal, detalhando as entidades, os seus atributos e as respectivas chaves primárias e estrangeiras.

No sistema proposto, a entidade utilizadores armazena as informações principais de acesso e identificação, tais como nome, email, senha e tipo de perfil. A partir desta entidade estão associados diferentes tipos de utilizadores, como cidadão, polícia, investigador e administrador, que possuem permissões específicas dentro da plataforma.

A entidade denúncias contém os dados relacionados com os casos de vitimização registados no sistema, incluindo informações como tipo de crime, data da ocorrência, localização, descrição do caso e estado da denúncia. Cada denúncia está associada a um utilizador que realizou o registo.

Além disso, a entidade dados de vitimização armazena os dados estatísticos provenientes de ficheiros Excel utilizados para análise da vitimização ao nível do sexo, ocupação e outros factores sociais. Esses dados são utilizados pelos investigadores para gerar relatórios e estatísticas.

O sistema também inclui a entidade notificações, responsável por armazenar mensagens enviadas automaticamente aos utilizadores sempre que ocorrem actualizações relevantes no sistema, como alterações no estado de uma denúncia ou publicação de novos dados.

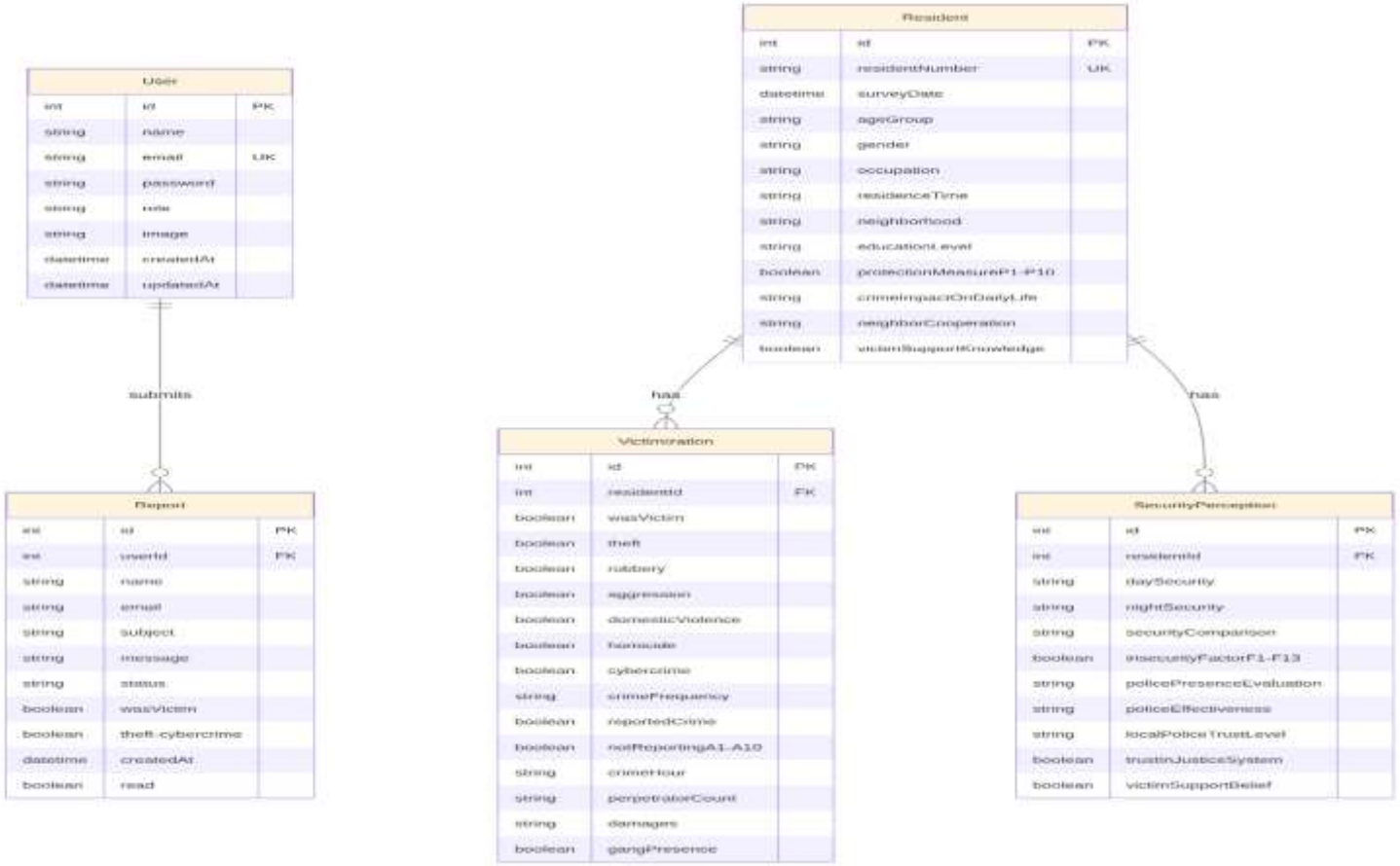
Outra entidade importante é o chatbot, que está associado à base de dados de vitimização e permite responder perguntas feitas pelos utilizadores com base nos dados armazenados.

Dessa forma, o diagrama ER representa a estrutura da base de dados do sistema, demonstrando como as diferentes entidades estão relacionadas e como os dados são organizados para suportar as funcionalidades da plataforma.

.

Figura 24.

Diagrama Entidade-Relacionamenro (ER)



Fonte: Elaborado pelo autor, 2026.

2.8 Diagrama de Actividade

este diagrama descreve de forma sequencial o fluxo de acções realizadas por um cidadão ao registar uma denúncia de vitimização na plataforma, desde o acesso ao sistema e autenticação até ao envio da denúncia, validação dos dados e confirmação do registo.

O processo inicia quando o utilizador acede à plataforma e efectua o login no sistema. Após a autenticação, o cidadão selecciona a opção de registar denúncia, sendo então apresentado um formulário onde deve inserir informações como tipo de crime, data da ocorrência, localização e descrição do caso.

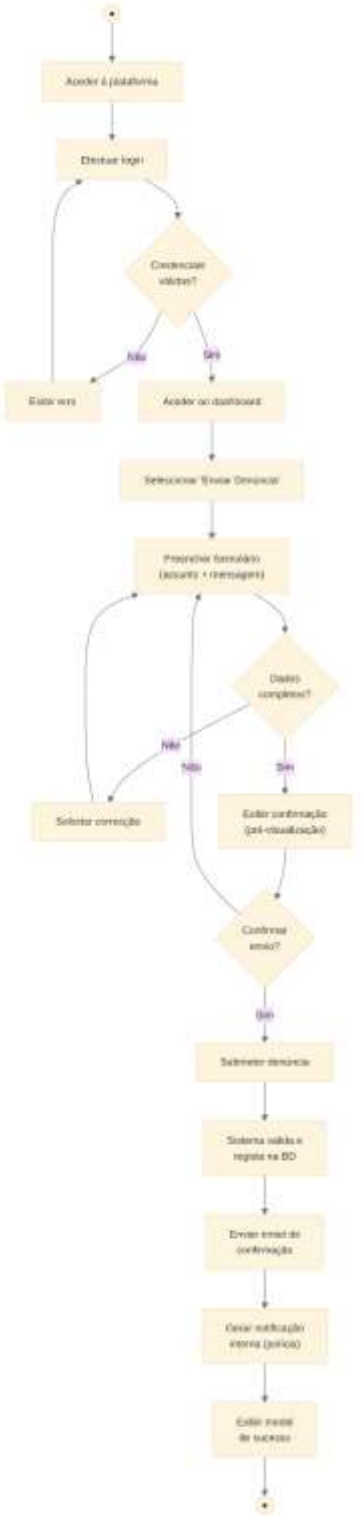
Depois de preencher os dados, o utilizador submete o formulário e o sistema procede à validação das informações introduzidas. Caso os dados estejam completos e correctos, a denúncia é registada na base de dados e o sistema apresenta uma mensagem de confirmação de sucesso, podendo também gerar uma notificação para acompanhamento do processo.

Caso sejam detectados dados incompletos ou inválidos, o sistema solicita ao utilizador que corrija as informações antes de finalizar o registo da denúncia. Este fluxo evidencia os pontos de decisão, mostrando os diferentes caminhos possíveis durante a execução do processo.

Dessa forma, o diagrama de actividade permite compreender de forma clara o fluxo de funcionamento do processo de registo de denúncias dentro da plataforma de análise de vitimização criminal.

Figura 25.

Diagrama de Actividade.



Fonte: Elaborado pelo autor, 2026.

2.9 Diagrama de Sequência

este diagrama apresenta a interacção dinâmica entre os diferentes elementos envolvidos no processo de registo de uma denúncia de vitimização criminal, nomeadamente o Cidadão (utilizador), Interface do Sistema, Sistema da Aplicação e Base de Dados. O diagrama demonstra a sequência de comunicação entre esses componentes durante o processo de acesso à plataforma e submissão de uma denúncia.

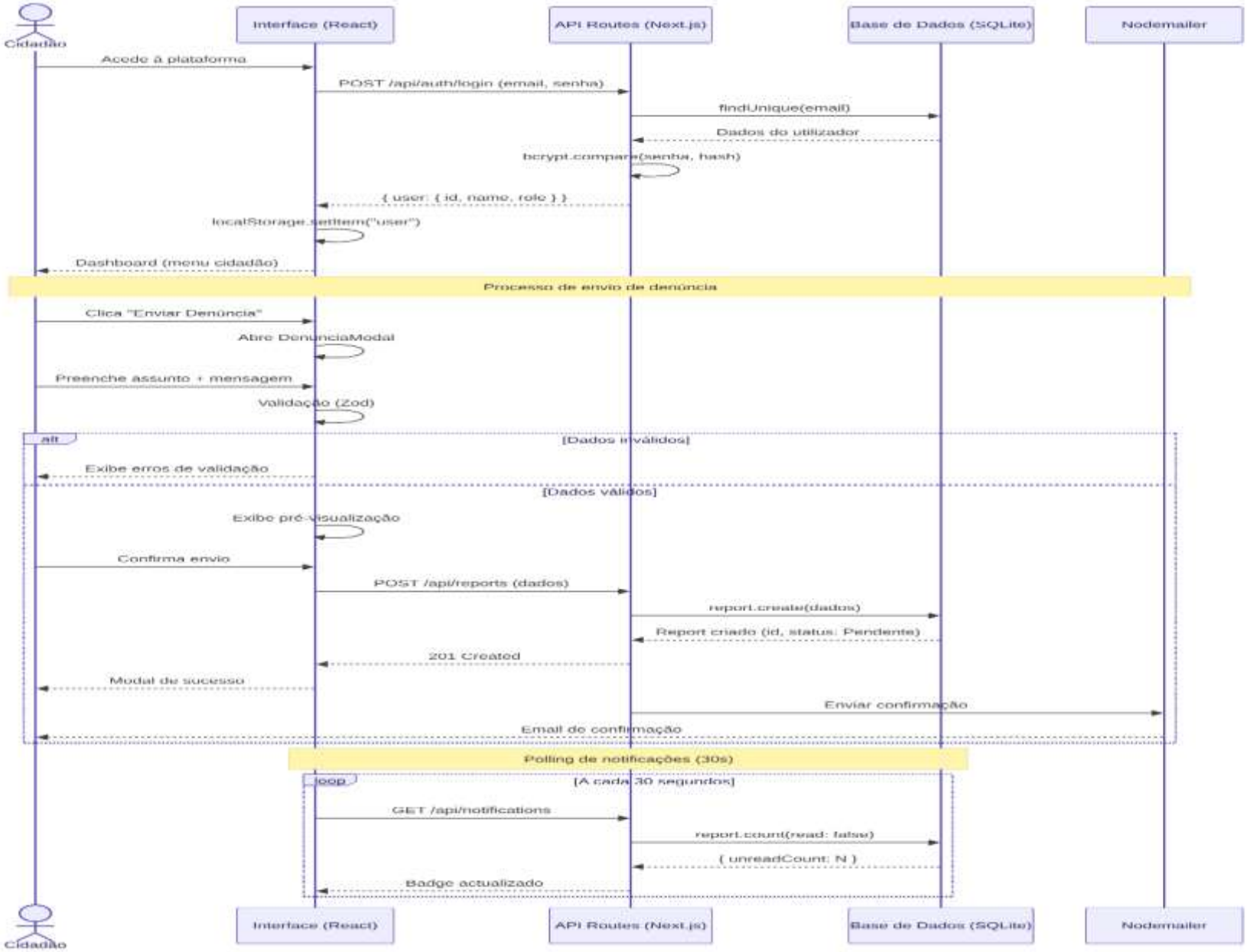
Inicialmente, o cidadão acede à plataforma e realiza o login através da interface do sistema. A interface envia as credenciais para o sistema da aplicação, que por sua vez verifica essas informações na base de dados. Caso os dados estejam correctos, o sistema autoriza o acesso do utilizador.

Após a autenticação, o cidadão preenche o formulário de denúncia de vitimização, inserindo informações como tipo de crime, data da ocorrência, localização e descrição do caso. A interface envia então esses dados ao sistema, que procede à validação das informações.

Se os dados forem válidos, o sistema envia as informações para a base de dados, onde a denúncia é registada. Em seguida, o sistema retorna uma resposta para a interface, informando ao utilizador que a denúncia foi submetida com sucesso. Caso existam erros ou dados incompletos, o sistema comunica a necessidade de correcção antes de finalizar o processo.

Dessa forma, o diagrama de sequência permite visualizar de forma clara a troca de mensagens entre os diferentes componentes do sistema e o comportamento do sistema em cada etapa do processo de registo de denúncias de vitimização criminal.

Figura 26.
Diagrama de Sequência .


Cidadão
Interface (React)
API Routes (Next.js)
Base de Dados (SQLite)
Nodemailer
Acede à plataforma
POST /api/auth/login (email, senha)
findUnique(email)
Dados do utilizador
bcrypt.compare(senha, hash)
{ user: { id, name, role } }
localStorage.setItem("user")
Dashboard (menu cidadão)
Processo de envio de denúncia
Clica "Enviar Denúncia"
Abre DenunciaModal
Preenche assunto + mensagem
Validação (Zod)
alt
[Dados inválidos]
Exibe erros de validação
[Dados válidos]
Exibe pré-visualização
Confirma envio
POST /api/reports (dados)
report.create(dados)
Report criado (id, status: Pendente)
201 Created
Modal de sucesso
Enviar confirmação
Email de confirmação
Polling de notificações (30s)
loop
[A cada 30 segundos]
GET /api/notifications
report.count(read: false)
{ unreadCount: N }
Badge actualizado
Cidadão
Interface (React)
API Routes (Next.js)
Base de Dados (SQLite)
Nodemailer

Fonte: Elaborado pelo autor, 2026

CONCLUSÃO

O presente trabalho teve como objectivo geral desenvolver uma plataforma digital com base na análise de inquéritos de vitimização criminal e percepção de segurança no município da Samba, no ano de 2025, visando contribuir para a melhoria da recolha e gestão de dados e para o fortalecimento das políticas públicas de segurança.

Em conformidade com o primeiro objectivo específico fundamentar, à luz da literatura, os conceitos de plataforma digital, inquérito de vitimização criminal e percepção de segurança constatou-se que a integração entre tecnologia e Ciências Criminais constitui uma estratégia contemporânea essencial para enfrentar os desafios da criminalidade urbana. A revisão teórica permitiu compreender que os inquéritos de vitimização são instrumentos fundamentais para revelar a chamada "cifra negra" da criminalidade, isto é, os crimes que não constam nos registos oficiais. Tal fundamentação mostrou-se coerente com os dados empíricos obtidos, uma vez que 68,8% das vítimas (Tabela 10) afirmaram não ter denunciado os crimes sofridos, sendo a falta de confiança na polícia (62,2%, Tabela 11) o principal motivo apontado. Esses resultados reforçam a relevância científica do estudo e demonstram a necessidade de mecanismos alternativos e estruturados de recolha de informação.

No que se refere ao segundo objectivo específico, programar uma plataforma digital para a análise de inquéritos de vitimização criminal e percepção de segurança verificou-se que a ferramenta desenvolvida permite organizar dados sociodemográficos, sistematizar informações sobre tipos de crime, frequência de vitimização e horários de ocorrência. Os resultados evidenciaram uma taxa de vitimização elevada (55,9%, Tabela 7), com predominância de crimes patrimoniais, nomeadamente roubo (69,5%) e furto (62,3%) conforme a Tabela 8. Observou-se ainda uma incidência significativa de revitimização (56,8%, Tabela 9), bem como maior ocorrência de crimes no período nocturno (62,3%, Tabela 12). A programação da plataforma possibilitou a centralização e cruzamento dessas variáveis, permitindo uma leitura integrada e estruturada da realidade criminal no bairro Gamek à Direita.

Relativamente ao terceiro objectivo específico, disponibilizar uma plataforma digital integrando os conhecimentos das Ciências Criminais e da Engenharia Informática constatou-se que a interdisciplinaridade adoptada no estudo constituiu um diferencial relevante. A conjugação entre fundamentos teóricos da vitimologia, análise estatística e desenvolvimento tecnológico permitiu criar um sistema capaz de gerar indicadores, apoiar a identificação de padrões e fornecer subsídios concretos para a tomada de decisão. A estruturação digital dos dados reduz a fragmentação informacional, melhora a acessibilidade e fortalece o planeamento estratégico de segurança pública.

Os resultados do estudo evidenciam que o município da Samba enfrenta desafios significativos no domínio da vitimização criminal, caracterizados por elevada incidência

de crimes patrimoniais, recorrência de vitimização e baixa taxa de denúncia. Tais elementos revelam fragilidades institucionais e a necessidade de políticas públicas mais orientadas por evidências empíricas e dados sistematizados.

Conclui-se, que os objectivos propostos foram alcançados, uma vez que a fundamentação teórica sustentou cientificamente o estudo, a plataforma foi devidamente programada e a sua disponibilização demonstrou potencial para melhorar a recolha, organização e análise de dados sobre vitimização criminal e percepção de segurança. A integração entre Ciências Criminais e Engenharia Informática mostrou-se adequada e pertinente ao contexto angolano, representando uma inovação relevante no domínio da gestão da informação criminal.

Referências Bibliográficas

Acs, Z. J., Song, A. K., Szerb, L., & Audretsch, D. B., & Komlósi, É. (2022). The evolution of the global digital platform economy: 1971–2021. Small Business Economics.

AGÊNCIA DE ESTATÍSTICA DE ANGOLA. (2025). Relatório síntese Censo 2024. https://censo2024.ine.gov.ao/Relatorio_Sintese_Censo2024.pdf

Alemika, E. E. O. (2015). Crime victimization and fear of crime in Africa. African Development Bank.

Araghi, S., Birch, P., Heggart, K., Buchanan, J., & Wallace, H. (2025). Digital community management for crime prevention and public safety: Strategies for safer and more inclusive online communities. Journal of Community Safety & Well-Being.

Citizen (app). (n.d.). Citizen app history and features. Wikipedia. https://en.wikipedia.org/wiki/Citizen_(app)

Ciberdúvidas. (2021). A morfologia do nome plataforma. https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/a-morfologia-da-plataforma/36403

Crowdmapping. (n.d.). Crowdmapping and collaborative crime data mapping. Wikipedia. https://en.wikipedia.org/wiki/Crowdmapping

de Reuver, M., Sørensen, C., & Basole, R. C. (2018). The digital platform: A research agenda. Journal of Information Technology, 33(2), 124–135. https://doi.org/10.1057/s41265-016-0033-3

Era da Informação. (n.d.). História da revolução digital. Wikipedia. https://pt.wikipedia.org/wiki/Era_da_Informa%C3%A7%C3%A3o

Evans, D. S., & Schmalensee, R. (2016). Matchmakers: The new economics of multisided platforms. Harvard Business Review Press.

Fattah, E. A. (2010). From crime policy to victim policy. Palgrave Macmillan.

Garland, D. (2001). The culture of control: Crime and social order in contemporary society. University of Chicago Press.

Gawer, A. (2021). Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. Long Range Planning, 54(5), 102045. https://doi.org/10.1016/j.lrp.2020.102045

Ha, S., & Kim, S. (2024). Developing a conceptual framework for digital platform literacy. Telecommunications Policy.

Hindelang, M. J., Gottfredson, M., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Ballinger.

Jackson, J., Bradford, B., Stanko, E., & Hohl, K. (2017). Just authority? Trust in the police in England and Wales. Routledge.

Killias, M., van Kesteren, J., & Mayhew, P. (2016). The International Crime Victims Survey (ICVS). Routledge.

Mendelsohn, B. (1956). Une nouvelle branche de la science bio-psycho-sociale: La victimologie. Revue Internationale de Criminologie.

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). Platform revolution: How networked markets are transforming the economy. W. W. Norton & Company.

Platform economy. (n.d.). História da economia de plataformas. Wikipedia. https://en.wikipedia.org/wiki/Platform_economy

Real-Time Crime Center. (n.d.). Real-Time Crime Center operations and data integration. Wikipedia. https://en.wikipedia.org/wiki/Real-Time_Crime_Center

Rewatkar, B., Choudhari, K., Godghate, P., & Uikey, R. (2024). Enhancing public safety with online crime reporting systems. International Journal of Advanced Research in Science, Communication and Technology.

Sampson, R. J. (2012). Great American city: Chicago and the enduring neighborhood effect. University of Chicago Press.

Shan, Y. (2026). Digital platforms and the transformation of crime governance. Journal of Chinese Sociology, 13(1).

Tiwana, A. (2014). Platform ecosystems: Aligning architecture, governance, and strategy. Morgan Kaufmann.

UNODC. (2010). Handbook on victimization surveys. United Nations Office on Drugs and Crime.

Van Dijk, J. (2015). The case for survey-based crime indicators. European Journal of Criminology, 12(4), 437–456.

Van Dijk, J., Van Kesteren, J., & Smit, P. (2014). Criminal victimisation in international perspective. Boom Lemma.

Web 2.0. (n.d.). História da Web 2.0 e evolução da internet. Wikipedia. https://en.wikipedia.org/wiki/Web_2.0

APÊNDICE

*Apêndice n.º 1 – **INQUÉRITO SOBRE VITIMIZAÇÃO CRIMINAL E PERCEPÇÃO DE SEGURANÇA**.*

I. DADOS SOCIODEMOGRÁFICOS

1.Idade:

18–25 anos ( ) 26–35 anos ( ) 36–45 anos ( ) 46–55 anos ( ) Mais de 55 anos ( )

2.Género:

Masculino ( ) Feminino ( )

3.Ocupação:

Trabalha ( ) Estuda ( ) Outra (especifique): _____

4.Tempo de residência no bairro Gamek à Direita:

Menos de 1 ano ( ) 1 a 3 anos ( ) 4 a 6 anos ( ) 7 a 10 anos ( ) Mais de 10 anos ( )

5.Localização no bairro (rua, quarteirão ou outra referência): _____

6.Nível de escolaridade:

Ensino Primário ( ) Ensino Secundário ( ) Ensino Superior ( )

II. EXPERIÊNCIAS DE VITIMIZAÇÃO CRIMINAL

7.Já foi vítima de algum crime no bairro Gamek à Direita nos últimos 12 meses?

Sim ( ) Não ( )

(Se sim, responda às próximas questões; se não, avance para a pergunta 15.)

8.Que tipo de crime ocorreu? (pode assinalar mais de uma opção)

- Furto
- Roubo ou assalto à mão armada
- Agressão física
- Arrombamento de residência
- Violência doméstica
- Homicídio ou tentativa de homicídio
- Estupro ou violência sexual
- Tráfico de drogas
- Vandalismo ou destruição de patrimônio
- Extorsão ou ameaças
- Sequestro ou cárcere privado
- Estelionato ou fraude
- Crime cibernético (golpes online, invasão de conta, etc.)
- Outros (especifique): _____

9. Quantas vezes foi vítima de crime nesse período?

1 vez ( ) 2 vezes ( ) 3 vezes ( ) 4 vezes ( ) 5 ou mais vezes ( )

10. O(s) crime(s) foi(ram) denunciado(s) às autoridades policiais?

Sim ( ) Não ( )

10.1. Se não, por que motivo? (pode assinalar mais de uma opção)

- Medo de represálias
- Falta de confiança na polícia
- Dificuldade de acesso às autoridades
- Sensação de inutilidade da denúncia
- Vergonha ou constrangimento
- .Desconhecimento sobre como denunciar
- Envolvimento pessoal com o agressor
- Receio de ser culpabilizado(a)
- Falta de provas ou testemunhas
- Outros (especifique): _____

Complemento — Detalhes do incidente:

11.Data e Hora do incidente:

- Ano: _____
- Mês: _____
- Horário aproximado: Manhã ( ) Tarde ( ) Noite ( )

12.Localização exata dentro do bairro:_____

13.Número de autores envolvidos: 1 ( ) 2 ( ) 3 ou mais ( )

14.Danos e consequências sofridas: (pode assinalar mais de uma opção)

- Materiais
- Físicos
- Psicológicos
- Outros (especifique): _____

III. PARTICIPAÇÃO DE GRUPOS ESPECÍFICOS EM CRIMES

15.Identifica a presença de gangues ou associações criminosas no bairro?

Sim ( ) Não ( ) Não sabe ( )

IV. PERCEPÇÃO DE SEGURANÇA

16.Como avalia a sua sensação de segurança ao circular no bairro durante o dia?

Muito seguro(a) ( ) Seguro(a) ( ) Nem seguro(a) ( ) Nem inseguro(a) ( ) Inseguro(a) ( ) Muito inseguro(a) ( )

17.Como avalia a sua sensação de segurança ao circular no bairro durante a noite?

Muito seguro(a) ( ) Seguro(a) ( ) Nem seguro(a) ( ) Nem inseguro(a) ( ) Inseguro(a) ( ) Muito inseguro(a) ( )

18.Comparado aos anos anteriores, a sua sensação de segurança:

Melhorou ( ) Permaneceu igual ( ) Piorou ( )

19.Quais áreas específicas do bairro você considera mais perigosas?_____

20.Em quais horários do dia você se sente mais inseguro(a)?

Manhã ( ) Tarde ( ) Noite ( ) Madrugada ( )

21.Na sua opinião, quais factores mais contribuem para a insegurança no bairro? (pode assinalar mais de uma opção)

- Falta de iluminação pública
- Ausência de policiamento frequente
- Áreas abandonadas ou degradadas
- Falta de organização comunitária
- Desemprego e dificuldades económicas
- Consumo e tráfico de drogas
- Conflitos entre grupos ou gangues
- Deficiências na infraestrutura urbana
- Falta de espaços de lazer e atividades para jovens
- Ineficiência da resposta policial
- Violência física e/ou sexual
- Violência doméstica
- Outros (especifique): _____

22.Você adoptou alguma medida de proteção extra por se sentir inseguro(a)? (pode assinalar mais de uma opção)

- Evitar sair à noite
- Reforçar fechaduras ou instalar alarmes
- Evitar andar sozinho(a) em certas áreas
- Mudar rotina ou trajeto diário
- Carregar item de defesa pessoal
- Participar de grupos de vigilância comunitária
- Pedir apoio de amigos, familiares ou vizinhos
- Contratar segurança privada
- Outras medidas: _____
- Não adoptou nenhuma medida

Apêndice n.º 2 – Questionário.

QUESTIONÁRIO CIENTÍFICO PARA LEVANTAMENTO DE REQUISITOS

Plataforma Digital de Recolha e Gestão de Dados de Vitimização Criminal e Percepção de Segurança

Este formulário tem como objectivo recolher informações junto de profissionais e instituições que lidam com dados de criminalidade, de modo a identificar as necessidades reais para o desenvolvimento de uma plataforma digital de recolha, gestão e análise de dados de vitimização criminal e percepção de segurança.

As informações recolhidas serão utilizadas exclusivamente para fins académicos no âmbito do Trabalho de Conclusão de Curso (TCC).

I. Identificação do Respondente

Nome: Celina Elizabeth José

Instituição: INSUTEC

Cargo/Função: Estudante

Área de actuação: Ciências Criminais

Contacto: 927878753

Data: 02/10/2025

II. Experiência com Dados de Criminalidade

1. Pode descrever brevemente o seu trabalho ou função na instituição?

R: Exerço a função de estudante na área de Ciências Criminais, desenvolvendo actividades académicas voltadas para o estudo da criminalidade, vitimização e percepção de segurança, com enfoque na análise de dados e desenvolvimento de soluções tecnológicas aplicadas à segurança pública.

2. A sua instituição realiza recolha ou registo de dados relacionados com criminalidade ou vitimização?

R: Sim, a instituição realiza recolha de dados no âmbito académico, através de inquéritos, pesquisas de campo e estudos científicos relacionados à vitimização criminal e percepção de segurança.

3. Que tipo de informações normalmente são recolhidas nesses registos?

R: São recolhidas informações como:

- Tipo de crime sofrido;
- Local e data da ocorrência;
- Perfil da vítima (idade, sexo, ocupação);
- Circunstâncias do crime;
- Percepção de segurança dos cidadãos;
- Frequência de ocorrência de crimes.

4. Como esses dados são actualmente armazenados ou organizados?

R: Os dados são armazenados principalmente em formatos manuais e digitais simples, como questionários físicos, documentos em Word planilhas em Excel e digitalização na google form, sem um sistema integrado de gestão.

5. Quais são as principais dificuldades enfrentadas no processo actual de registo ou gestão desses dados?

R: As principais dificuldades incluem:

- Falta de padronização na recolha de dados;
- Dificuldade na organização e centralização das informações;
- Risco de perda de dados;
- Limitação na análise estatística;
- Demora na geração de relatórios;
- Baixa eficiência na consulta de informações.

III. Necessidade de um Sistema Digital

1. Na sua opinião, qual seria a importância de uma plataforma digital para recolha e gestão de dados de vitimização criminal?

R: A plataforma digital seria fundamental para melhorar a eficiência, organização e segurança dos dados, permitindo uma análise mais rápida e precisa, além de apoiar a tomada de decisões estratégicas na área de segurança pública.

2. Que problemas actuais poderiam ser resolvidos com a implementação de um sistema digital?

- Redução da perda de dados;
- Melhoria na organização e armazenamento;
- Automatização de processos;
- Facilidade na geração de relatórios;
- Melhor acesso e partilha de informações;
- Aumento da confiabilidade dos dados.

3. Que tipo de informação considera essencial que o sistema permita registar?

- Dados pessoais da vítima (com protecção);
- Tipo de crime;
- Localização geográfica da ocorrência;
- Data e hora;
- Descrição do incidente;
- Nível de percepção de segurança;
- Frequência de vitimização;
- Dados estatísticos agregados.

IV. Funcionalidades Desejadas no Sistema

1. Que funcionalidades ou ferramentas considera importantes que o sistema possua?

- Cadastro de dados de vítimas e ocorrências;
- Visualização gráfica (gráficos e dashboards);
- Georreferenciamento (mapas);
- Exportação de dados;
- Backup automático.

2. O sistema deveria permitir realizar que tipos de operações com os dados (por exemplo: inserir, consultar, actualizar, gerar relatórios, entre outras)?

- Inserir dados;
- Consultar informações;
- Actualizar registros;
- Eliminar dados (com controlo);
- Exportar dados.

3. Que tipo de relatórios ou análises considera úteis para apoiar o trabalho da sua instituição?

- Relatórios de incidência criminal por área;
- Estatísticas por tipo de crime;
- Análise temporal (mensal/anual);
- Perfil das vítimas;
- Índices de vitimização e percepção de segurança.

4. Considera importante que o sistema apresente gráficos, estatísticas ou mapas para análise dos dados? Explique.

R: Sim, é extremamente importante, pois facilita a interpretação dos dados, permitindo identificar padrões, tendências e áreas críticas de criminalidade de forma visual e intuitiva.

V. Utilização e Acesso ao Sistema

1. Quem seriam os principais utilizadores do sistema?

- Investigadores;
- Estudantes;
- Técnicos de análise de dados;
- Instituições de segurança pública;
- Cidadão.

2. Acha importante que existam diferentes níveis de acesso (exemplo: administrador, técnico, utilizador)?

R: Sim, é essencial para garantir a segurança e controlo dos dados, permitindo que cada utilizador tenha acesso apenas às informações necessárias conforme sua função.

3. Em que dispositivos o sistema deveria funcionar?

- Computadores;
- Tablets;
- Telemóveis (smartphones).

4. Que características considera importantes para que o sistema seja fácil de utilizar?

- Interface simples;
- Navegação clara;
- Rapidez no acesso às informações;
- Linguagem acessível;
- Design responsivo.

VI. Segurança e Protecção dos Dados

1. Que cuidados considera necessários para garantir a segurança das informações registadas no sistema?

- Criptografia de dados;
- Autenticação de utilizadores;
- Controlo de acesso por níveis;
- Backups regulares;
- Monitoramento de acesso.

2. Que tipo de dados considera sensíveis e que devem ter maior nível de protecção?

- Dados pessoais das vítimas;
- Endereços;

- Contactos;
- Informações sobre ocorrências específicas;
- Identidade dos envolvidos.

VII. Integração com Inteligência Artificial

1. O sistema poderá incluir um Chatbot Inteligente de Vitimização, capaz de responder perguntas e auxiliar na consulta de dados. Na sua opinião, como esse recurso poderia ajudar os utilizadores?

R: O Perito em Análise poderia auxiliar na consulta rápida de informações, responder dúvidas frequentes, orientar o preenchimento de dados e facilitar o acesso a estatísticas e relatórios.

2. Que tipo de perguntas ou informações considera que o Perito em Análise deveria ser capaz de responder?

- Quantos crimes ocorreram em determinada área?
- Qual o tipo de crime mais frequente?
- Estatísticas por período
- Nível de segurança de uma zona
- Informações gerais sobre vitimização

VIII. Sugestões e Recomendações

Caso tenha outras sugestões para melhorar a plataforma digital proposta, por favor descreva abaixo:

- Seja de fácil acesso e utilização;
- Inclua funcionalidades de análise avançada;
- Permita integração com outras instituições;
- Utilize inteligência artificial para apoio à decisão;
- Garanta alta segurança dos dados;
- Seja constantemente actualizada.

Apêndice n.º 2 – Histórias de Usuários. Requisitos e Diagramas.

HISTÓRIAS DE USUÁRIO, REQUISITOS E DIAGRAMAS

O presente documento extrai as histórias de usuário (user stories) implícitas no código-fonte da plataforma SafeAngola, deriva os requisitos funcionais e não funcionais, e apresenta os diagramas de classes e entidade-relacionamento.

1. Histórias de Usuário (User Stories)

As histórias de usuário foram extraídas a partir da análise do código-fonte do repositório, nomeadamente das páginas do dashboard (layout.tsx com menus diferenciados por perfil), das rotas de API, dos componentes de interface e do motor pericial Python. Cada história segue o formato: Como [actor], quero [acção], para que [objectivo].

ID	Actor	Quero...	Para que...
US01	Cidadão	Registar-me na plataforma com nome, email, senha e perfil	Possa aceder às funcionalidades da plataforma
US02	Utilizador	Efectuar login com email e senha	Aceda ao painel correspondente ao meu perfil
US03	Utilizador	Recuperar a minha senha via email	Possa aceder novamente à minha conta
US04	Utilizador	Editar o meu perfil (nome, email, foto)	As minhas informações estejam actualizadas
US05	Cidadão	Enviar uma denúncia pública ou anónima	O crime seja registado mesmo sem ir à esquadra
US06	Cidadão	Consultar o estado das minhas denúncias	Saiba se estão a ser acompanhadas
US07	Polícia	Visualizar e filtrar todas as ocorrências recebidas	Possa priorizar e acompanhar os casos
US08	Polícia	Actualizar o estado de uma denúncia	O cidadão saiba o progresso da investigação
US09	Admin	Importar dados de inquéritos via ficheiro Excel	Os dados fiquem centralizados na plataforma

US10	Investigador	Visualizar gráficos interactivos de vitimização	Identifique padrões e tendências criminais
US11	Investigador	Filtrar dados por bairro, género, idade e tipo de crime	Faça análises segmentadas
US12	Investigador	Comparar percepções de segurança entre grupos	Compreenda diferenças de experiência
US13	Investigador	Gerar e exportar relatórios em PDF/Excel	Documente e partilhe os resultados
US14	Investigador	Fazer perguntas em linguagem natural ao chatbot	Obtenha análises estatísticas sem saber programar
US15	Cidadão	Consultar o chatbot sobre segurança no meu bairro	Tome decisões informadas sobre protecção
US16	Admin	Gerir utilizadores (criar, editar, remover, atribuir perfis)	Controle quem acede à plataforma
US17	Admin	Realizar backup e restauração da base de dados	Os dados estejam protegidos contra perdas
US18	Admin	Gerir a base de dados (visualizar, limpar dados)	Mantenha a integridade dos dados
US19	Cidadão	Procurar serviços de apoio às vítimas	Saiba onde obter ajuda
US20	Utilizador	Alternar entre tema claro e escuro	Tenha conforto visual ao usar a plataforma
US21	Polícia	Receber notificações de novas denúncias	Responda rapidamente às ocorrências
US22	Investigador	Lançar inquéritos de vitimização directamente na plataforma	Não dependa apenas de ficheiros Excel

2. Requisitos Funcionais (RF)

Os requisitos funcionais foram derivados das histórias de usuário e validados contra a implementação real no código-fonte:

ID	Requisito	Descrição	US
RF01	Cadastro de utilizador	Registo com nome, email, senha e perfil (ADMIN, RESEARCHER, POLICE, CITIZEN); valida email único; senha com hash bcrypt; email de boas-vindas enviado	US01
RF02	Login por perfil	Autenticação por email/senha; menu lateral diferenciado por perfil (admin: 11 itens, researcher: 12, police: 6, citizen: 6); rotas protegidas	US02
RF03	Recuperação de senha	Envio de link de recuperação por email via nodemailer	US03

RF04	Gestão de perfil	Edição de nome, email e foto (upload base64); validação de email duplicado; persistência imediata	US04
RF05	Envio de denúncias	Formulário com assunto e mensagem (obrigatórios), nome e email (opcionais para anonimato); passo de confirmação antes do envio; modal de sucesso	US05
RF06	Consulta de denúncias	Listagem filtrada por userId para cidadãos; ordenação por data; exibição de estado actual	US06
RF07	Gestão de ocorrências	Listagem completa para polícia/admin; marcação como lida (PUT read); actualização de estado (Pendente→Em Análise→Encaminhado→Resolvido)	US07,US08
RF08	Notificações	Contagem de denúncias não lidas via polling (/api/notifications); ícone NotificationBell no header do dashboard	US21
RF09	Importação Excel	Upload de .xlsx via ExcelJS; validação de estrutura (103 colunas); importação transacional com rollback; relatório de erros	US09
RF10	Lançamento de inquéritos	Formulário de entrada directa de dados de vitimização na plataforma (página data-entry)	US22
RF11	Dashboards estatísticos	12 endpoints dedicados com gráficos Recharts: crimes-by-neighborhood, victimization-by-age-and-gender, victimization-by-crime-type, reasons-for-not-reporting, day-night-security, police-trust, security-perception-by-gender, security-perception-vs-police-presence, occupation-victim, victimization-by-education-level, residents-by-age-group, summary	US10
RF12	Filtros e consultas	Filtragem por bairro, género, faixa etária, tipo de crime e outros critérios; páginas data-filter e data-query	US11
RF13	Comparação de percepções	Página perception-comparison para análise cruzada de percepção de segurança entre grupos demográficos	US12
RF14	Relatórios e exportação	Geração de relatórios via página report-creation; exportação em PDF/Excel/Imagem; endpoint /api/reports	US13
RF15	Chatbot inteligente	Interface ChatbotInterface.tsx; consultas em linguagem natural; integração com motor pericial Python via API; respostas baseadas em dados reais com métodos estatísticos	US14,US15
RF16	Gestão de utilizadores	CRUD completo: GET (listar), PUT (editar), DELETE (remover); atribuição de perfis; página dashboard/users	US16

RF17	Backup e restauração	Página dashboard/backup para criação e restauração de cópias da base de dados SQLite	US17
RF18	Gestão da base de dados	Página database-management para visualização e manutenção dos dados armazenados	US18
RF19	Serviços de apoio	Página /apoio com listagem de 6 categorias de serviços (Polícia, IGAE/INAC/SIC, Psicologia, Assistência Social, Gabinetes Jurídicos, ONGs)	US19
RF20	Tema claro/escuro	Alternância via next-themes com ThemeToggle no header; persistência da preferência	US20

3. Requisitos Não Funcionais (RNF)

Os requisitos não funcionais foram identificados a partir da análise da arquitectura, das dependências (package.json), do Dockerfile, do schema Prisma e das práticas de codificação observadas:

ID	Categoria	Descrição e Evidência no Código
RNF01	Segurança	Senhas armazenadas com hash bcrypt (bcryptjs); protecção de rotas por perfil; validação de email único; API tokens com hash SHA-256 no motor pericial
RNF02	Escalabilidade	Dockerfile multi-estágio (deps→builder→runner) com docker-compose; arquitectura preparada para réplicas horizontais
RNF03	Usabilidade	Interface com shadcn-ui/Radix UI (acessibilidade nativa); menus diferenciados por perfil; mensagens de erro amigáveis (toast via Sonner); modais de confirmação
RNF04	Performance	React Query (@tanstack/react-query) para cache e sincronização; Next.js SSR/SSG para carregamento rápido; polling de 30s para notificações (não websocket)
RNF05	Portabilidade	Containerização Docker; SQLite como BD portátil (ficheiro único); compatibilidade cross-browser via Next.js
RNF06	Manutenibilidade	TypeScript para tipagem estática; Prisma ORM com schema declarativo e migrações versionadas (6 migrações); componentes reutilizáveis; separação front/back
RNF07	Integridade de dados	Transacções com rollback na importação Excel; validação Zod nos formulários; chaves primárias auto-incrementais; relações com integridade referencial (FK)

RNF08	Privacidade	Denúncias anónimas (nome/email opcionais); dados pessoais não expostos nas APIs públicas; select específico nos queries (exclui password)
RNF09	Acessibilidade	Radix UI com primitivas WCAG; labels em formulários; contraste via Tailwind; navegação por teclado; tema claro/escuro
RNF10	Responsividade	Tailwind CSS com classes responsivas (md:, lg:); layout flex/grid adaptativo; sidebar colapsável no dashboard
RNF11	Internacionalização	Interface em Português; motor pericial com respostas em Português; suporte multilingue preparado na arquitectura
RNF12	Backup e recuperação	Módulo de backup/restauração da BD SQLite; ficheiro único facilita cópia e transferência
RNF13	Extensibilidade	API RESTful do motor pericial com tokens (permite integração externa); modelos Prisma extensíveis; componentes modulares
RNF14	Comunicação	Envio automático de emails via nodemailer (boas-vindas, recuperação de senha, confirmação de denúncia)

4. Matriz de Rastreabilidade US → RF → Implementação

A seguinte matriz demonstra a rastreabilidade entre as histórias de usuário, os requisitos funcionais e os artefactos de código que os implementam:

US	RF	Artefacto de Código	Estado
US01	RF01	src/app/api/auth/register/route.ts + auth/register/page.tsx	Implementado e validado
US02	RF02	src/app/api/auth/login/route.ts + dashboard/layout.tsx (menus)	Implementado e validado
US05	RF05	DenunciaModal.tsx + /api/reports POST	Implementado e validado
US07	RF07	/api/occurrences GET/PUT + dashboard/occurrences/page.tsx	Implementado e validado
US09	RF09	ExcelUpload.tsx + /api/upload-excel/route.ts (283 linhas)	Implementado e validado
US10	RF11	GraphDisplay.tsx + 12 endpoints em /api/data/*	Implementado e validado
US14	RF15	ChatbotInterface.tsx + /api/chatbot + icriminalidade/indice.py	Implementado e validado
US16	RF16	/api/auth/users GET/PUT/DELETE + dashboard/users/page.tsx	Implementado e validado
US19	RF19	src/app/apoio/page.tsx (6 serviços listados)	Implementado e validado
US21	RF08	NotificationBell.tsx + /api/notifications (polling 30s)	Implementado e validado

5. Diagrama de Classes

O diagrama de classes representa a estrutura lógica do sistema SafeAngola, derivado directamente do schema Prisma (prisma/schema.prisma) e das classes Python do motor pericial (icriminalidade/indice.py). O diagrama segue a notação UML e apresenta as classes, seus atributos, métodos e relacionamentos.

5.1 Classes do modelo de dados (Prisma)

Classe: User

Atributos: id: Int [PK, auto], name: String?, email: String [unique], password: String, role: String [default: RESEARCHER], image: String?, createdAt: DateTime, updatedAt: DateTime

Métodos: register(name, email, password, role), login(email, password), updateProfile(name, email, image), resetPassword(email)

Notas: O atributo role admite os valores: ADMIN, RESEARCHER, POLICE, CITIZEN. O password é armazenado com hash bcrypt.

Classe: Resident

Atributos: id: Int [PK, auto], residentNumber: String [unique], surveyDate: DateTime?, ageGroup: String, gender: String, occupation: String, residenceTime: String, neighborhood: String, educationLevel: String, school: String?, emailContact: String?, protectionMeasureP1..P10: Boolean?, crimeImpactOnDailyLife: String?, neighborCooperation: String?, communityInitiativeParticipation: String?, securityImprovementSuggestions: String?, victimSupportServicesKnowledge: Boolean?, ...campos complementares

Relações: victimizations: Victimization[] (1:N), securityPerceptions: SecurityPerception[] (1:N)

Notas: Mapeia a Secção I do inquérito. Campos P1-P10 correspondem às medidas de protecção adoptadas.

Classe: Victimization

Atributos: id: Int [PK], residentId: Int [FK→Resident], wasVictim: Boolean, crimeGeneral: String?, theft: Boolean?, robbery: Boolean?, aggression: Boolean?, burglary: Boolean?, domesticViolence: Boolean?, homicide: Boolean?, rape: Boolean?, drugTrafficking: Boolean?, vandalism: Boolean?, extortion: Boolean?, kidnapping: Boolean?, fraud: Boolean?, cybercrime: Boolean?, otherCrime: String?, crimeFrequency: String, reportedCrime: Boolean, notReportingReasonA1..A10: Boolean?, crimeYear: Int?, crimeMonth: String?, crimeHour: String?, crimeLocation: String?, perpetratorCount: String, damages: String?, minorsInvolved: Boolean, crimesByWomen: Boolean, crimesAgainstWomen: Boolean, gangPresence: Boolean

Relações: resident: Resident (N:1)

Notas: Mapeia as Secções II e III do inquérito. 13 campos booleanos para tipos de crime, 10 para motivos de não denúncia.

Classe: SecurityPerception

Atributos: id: Int [PK], residentId: Int [FK→Resident], daySecurity: String, nightSecurity: String, securityComparison: String?, mostDangerousAreas: String?, mostInsecureHours: String?, insecurityFactorF1..F13: Boolean?, crimeFrequencyPerceptionGeneral: String?, crimeFrequencyPerceptionA..C: String?, crimeGravityPerception: String?, policePresenceEvaluation: String?, policeResponseSpeedEvaluation: String?, policeEffectivenessEvaluation: String?, localPoliceTrustLevel: String?, personalPoliceInteraction: String?, trustInPoliceAndJusticeSystem: Boolean?, victimSupportBelief: Boolean?

Relações: resident: Resident (N:1)

Notas: Mapeia a Secção IV do inquérito. 13 campos booleanos para factores de insegurança.

Classe: Report

Atributos: id: Int [PK], userId: Int?, name: String?, email: String?, subject: String, message: String, status: String [default: Pendente], age: String?, gender: String?, occupation: String?, educationLevel: String?, residenceTime: String?, neighborhood: String?, wasVictim: Boolean?, crimeTypes: String?, theft..cybercrime: Boolean?, otherCrime: String?, createdAt: DateTime, read: Boolean [default: false]

Métodos: create(data), updateStatus(id, status), markAsRead(id)

Notas: userId é opcional (permite denúncias anónimas). status admite: Pendente, Em Análise, Encaminhado, Resolvido.

5.2 Classes do motor pericial (Python)

Classe: PreProcessadorCriminal

Tipo: Classe utilitária (métodos de classe)

Métodos: processar(df) → DataFrame — limpa, organiza e enriquece os dados dos inquéritos, criando variáveis derivadas como índice de risco por bairro, categoria de risco e scores de severidade

Classe: MotorPericial

Atributos: df: DataFrame, CRIMES: list, MOTIVOS: list

Métodos: perfil_vitimizacao() → dict, analise_denuncia() → dict, analise_percepcao_seguranca() → dict, analise_institucional() → dict, analise_causal_social() → dict, matriz_correlacoes_chave() → dict, gerar_contexto_completo() → str

Métodos estatísticos internos: _safe_pearson(x, y), _interpretar_r(r), _safe_chi2(col1, col2), _group_comparison(cat_col, num_col)

Classe: DataManager

Atributos: df: DataFrame, df_raw: DataFrame, motor: MotorPericial, url: String

Métodos: load_data(local_fallback) → void, processar_grafico(config) → dict

5.3 Relacionamentos entre classes

User ←→ Report: Um utilizador pode criar várias denúncias (1:N, opcional — userId pode ser null para denúncias anónimas).

Resident ←→ Victimization: Um residente pode ter vários registos de vitimização (1:N obrigatório — residentId é FK não nula).

Resident ←→ SecurityPerception: Um residente pode ter vários registos de percepção de segurança (1:N obrigatório).

DataManager ←→ PreProcessadorCriminal: DataManager utiliza PreProcessadorCriminal para processar os dados (dependência).

DataManager ←→ MotorPericial: DataManager instancia e mantém referência ao MotorPericial (composição).

MotorPericial ←→ Google Gemini API: MotorPericial envia contexto estatístico para a IA e recebe respostas (dependência externa).

6. Diagrama Entidade-Relacionamento (ER)

O diagrama ER descreve a organização física dos dados na base de dados SQLite, derivado directamente do ficheiro prisma/schema.prisma. O diagrama apresenta as entidades, seus atributos com tipos de dados, chaves primárias (PK), chaves estrangeiras (FK) e os relacionamentos com cardinalidade.

6.1 Entidade: User

id: INTEGER [PK, AUTOINCREMENT] | name: TEXT [NULLABLE] | email: TEXT [UNIQUE, NOT NULL] | password: TEXT [NOT NULL] | role: TEXT [NOT NULL, DEFAULT 'RESEARCHER'] | image: TEXT [NULLABLE] | createdAt: DATETIME [DEFAULT NOW] | updatedAt: DATETIME [AUTO]

6.2 Entidade: Resident

id: INTEGER [PK, AUTOINCREMENT] | residentNumber: TEXT [UNIQUE, NOT NULL] | surveyDate: DATETIME [NULLABLE] | ageGroup: TEXT [NOT NULL] | gender: TEXT [NOT NULL] | occupation: TEXT [NOT NULL] | residenceTime: TEXT [NOT NULL] | neighborhood: TEXT [NOT NULL] | educationLevel: TEXT [NOT NULL] | school: TEXT | emailContact: TEXT | protectionMeasureP1..P10: BOOLEAN | crimeImpactOnDailyLife: TEXT | neighborCooperation: TEXT | communityInitiativeParticipation: TEXT | securityImprovementSuggestions: TEXT | victimSupportServicesKnowledge: BOOLEAN | ... (30 campos total)

6.3 Entidade: Victimization

id: INTEGER [PK, AUTOINCREMENT] | residentId: INTEGER [FK → Resident.id, NOT NULL] | wasVictim: BOOLEAN [NOT NULL] | theft..cybercrime: BOOLEAN (13 campos) | crimeFrequency: TEXT [NOT NULL] | reportedCrime: BOOLEAN [NOT NULL] | notReportingReasonA1..A10: BOOLEAN (10 campos) | crimeYear: INTEGER | crimeMonth: TEXT | crimeHour: TEXT | crimeLocation: TEXT | perpetratorCount: TEXT [NOT NULL] | damages: TEXT | minorsInvolved: BOOLEAN [NOT NULL] | gangPresence: BOOLEAN [NOT NULL] | ... (35 campos total)

6.4 Entidade: SecurityPerception

id: INTEGER [PK, AUTOINCREMENT] | residentId: INTEGER [FK → Resident.id, NOT NULL] | daySecurity: TEXT [NOT NULL] | nightSecurity: TEXT [NOT NULL] | securityComparison: TEXT | insecurityFactorF1..F13: BOOLEAN (13 campos) | policePresenceEvaluation: TEXT | policeResponseSpeedEvaluation: TEXT | policeEffectivenessEvaluation: TEXT | localPoliceTrustLevel: TEXT | trustInPoliceAndJusticeSystem: BOOLEAN | victimSupportBelief: BOOLEAN | ... (28 campos total)

6.5 Entidade: Report

id: INTEGER [PK, AUTOINCREMENT] | userId: INTEGER [FK → User.id, NULLABLE] | name: TEXT | email: TEXT | subject: TEXT [NOT NULL] | message: TEXT [NOT NULL] | status: TEXT [NOT NULL, DEFAULT 'Pendente'] | age: TEXT | gender: TEXT | occupation: TEXT | educationLevel: TEXT | residenceTime: TEXT | neighborhood: TEXT | wasVictim: BOOLEAN | theft..cybercrime: BOOLEAN (7 campos) | otherCrime: TEXT | createdAt: DATETIME [DEFAULT NOW] | read: BOOLEAN [DEFAULT FALSE] | ... (18 campos total)

6.6 Relacionamentos

Entidade Origem	Entidade Destino	Cardinalidade	FK
Resident	Victimization	1 : N	Victimization.residentId
Resident	SecurityPerception	1 : N	SecurityPerception.residentId
User	Report	1 : N (opcional)	Report.userId (nullable)

O diagrama evidencia que o sistema possui duas sub-redes de dados: (1) a rede de inquéritos, centrada na entidade Resident que se relaciona com Victimization e SecurityPerception, representando os dados recolhidos na investigação criminológica; e (2) a rede de operações, onde User se relaciona opcionalmente com Report, representando as funcionalidades de denúncia e gestão da plataforma. As duas sub-redes não possuem relação directa entre si no schema actual, o que reflecte a separação lógica entre os dados históricos dos inquéritos e os dados operacionais da plataforma.

Apêndice n.º 2 – Algumas telas da plataforma web.