

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
DE MINAS GERAIS – CAMPUS OURO BRANCO
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

GUILHERME HENRIQUE COSTA VIEIRA

**DESENVOLVIMENTO DE DISPOSITIVO DISCRETO DE ACIONAMENTO DE
EMERGÊNCIA PARA MULHERES EM SITUAÇÃO DE VIOLÊNCIA DOMÉSTICA:
ARQUITETURA, PROTOTIPAGEM E MODELO DE DISTRIBUIÇÃO**

OURO BRANCO
2026

GUILHERME HENRIQUE COSTA VIEIRA

**DESENVOLVIMENTO DE DISPOSITIVO DISCRETO DE ACIONAMENTO DE
EMERGÊNCIA PARA MULHERES EM SITUAÇÃO DE VIOLÊNCIA DOMÉSTICA:
ARQUITETURA, PROTOTIPAGEM E MODELO DE DISTRIBUIÇÃO**

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais – Campus Ouro Branco, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Jânio Rosa da Silva

V658d Vieira, Guilherme Henrique Costa.

Desenvolvimento de dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica: arquitetura, prototipagem e modelo de distribuição. /Guilherme Henrique Costa Vieira. – 2026.

19 f. il.col.

Orientador: Jânio Rosa da Silva.

Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal de Minas Gerais. *Campus* Ouro Branco, 2026.

1. Violência doméstica. 2. Dispositivo de emergência. 3. Internet das coisas (IoT). 4. Lei Maria da Penha. 5. Prototipagem de hardware. I. Vieira, Guilherme Henrique Costa. II. Silva, Jânio Rosa da. III. Instituto Federal de Minas Gerais. *Campus* Ouro Branco. IV. Título.

CDU. 004.42

Catalogação: Márcia Margarida Vilaça - CRB-6/2235
Biblioteca do Instituto Federal de Minas Gerais, *Campus* Ouro Branco



**MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE
MINAS GERAIS
CAMPUS OURO BRANCO**

Av. Afonso Sardinha, nº 90, Bairro Pioneiros, CEP: 36.420-000, Ouro Branco - Minas
Gerais - (31) 3742-2149 – gabinete.ourobranco@ifmg.edu.br

ANEXO II – ATA DE CONCLUSÃO DE TCC

Aos **14** dias do mês de **Julho** de **2026**, às **19:00** horas, **Guilherme Henrique Costa Vieira**, aluno(a) regularmente matriculado no Curso de Sistemas de Informação do Instituto Federal de Minas Gerais, campus Ouro Branco, matrícula **0100789**, concluiu o seu Trabalho de Conclusão de Curso por meio de:

() Publicação do artigo intitulado ____ na revista/conferência ____, cujo comprovante de aceitação será anexado a esta ata, recebendo a nota _____ pelo trabalho. Eu, na qualidade de orientador do aluno, lavrei a presente ata atestando a conclusão do trabalho, a qual será assinada por mim e pelo aluno.

Professor Orientador: _____

Aluno: _____

(**X**) Defesa em sessão pública realizada às **19:00** horas, na sala **do Google Meetings** do Instituto Federal de Minas Gerais, campus Ouro Branco, na presença da banca examinadora composta pelos docentes:

1 - Adilson Ribeiro de Oliveira

2 - Joaquim Eduardo de Moura

3 - Janio Rosa da Silva

do artigo intitulado **Dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica**



**MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE
MINAS GERAIS
CAMPUS OURO BRANCO**

Av. Afonso Sardinha, nº 90, Bairro Pioneiros, CEP: 36.420-000, Ouro Branco - Minas
Gerais - (31) 3742-2149 – gabinete.ourobranco@ifmg.edu.br

A banca examinadora, após reunião em sessão reservada, deliberou pela **Aprovação** do referido trabalho, atribuindo a nota **100,00**. Eu, na qualidade de presidente da banca examinadora, lavrei a presente ata que será assinada por mim, pelos demais examinadores e pelo aluno.

**NOME E ASSINATURA DOS COMPONENTES DA BANCA E DO
ORIENTADO**

Orientador: Janio Rosa da Silva

Examinador 1: Adilson Ribeiro de Oliveira

Examinador 2: Joaquim Eduardo de Moura

Aluno: Guilherme Henrique Costa Vieira

RESUMO

A violência doméstica contra a mulher persiste como problema estrutural no Brasil, com índices de feminicídio em ascensão mesmo diante do arcabouço jurídico instituído pela Lei Maria da Penha. As ferramentas atuais de resposta emergencial, como o Botão do Pânico, apresentam limitações operacionais quanto à discrição, autonomia e cobertura, que comprometem sua efetividade em cenários de coabitação com o agressor. Este trabalho propõe o desenvolvimento de um dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica, integrando arquitetura de hardware, prototipagem funcional e um modelo de distribuição articulado com a rede de proteção. A metodologia compreende a revisão bibliográfica sobre violência contra a mulher e tecnologias de proteção existentes, o levantamento de requisitos funcionais e não funcionais, o projeto da arquitetura de hardware e software do dispositivo, a construção de um protótipo funcional e a proposição de um modelo de distribuição integrado às delegacias especializadas (DEAMs) e aos centros de referência (CRAMs). Espera-se que o dispositivo proposto supere as limitações de discrição e cobertura das soluções atuais, oferecendo uma alternativa viável, de baixo custo e escalável para o acionamento emergencial rápido por mulheres em situação de violência doméstica, contribuindo com as políticas públicas de proteção.

Palavras-chave: Violência doméstica. Dispositivo de emergência. Internet das Coisas (IoT). Lei Maria da Penha. Prototipagem de hardware.

ABSTRACT

Domestic violence against women remains a structural problem in Brazil, with femicide rates rising despite the legal framework provided by the Maria da Penha Law. Existing emergency response tools, such as the Panic Button, present operational limitations regarding discretion, autonomy, and coverage that restrict their effectiveness in cohabitation scenarios. This work proposes the development of a discreet emergency activation device for women experiencing domestic violence, integrating hardware architecture, functional prototyping, and a distribution model articulated with the protection network. The methodology comprises a literature review on violence against women and existing protection technologies, the specification of functional and non-functional requirements, the design of the device's hardware/software architecture, the construction of a functional prototype, and the proposition of a distribution model integrated with specialized police stations (DEAMs) and reference centers (CRAMs). It is expected that the proposed device will overcome the discretion and coverage limitations of current solutions, providing a viable, low-cost, and scalable alternative for rapid emergency triggering by women in situations of domestic violence, contributing to public protection policies.

Keywords: Domestic violence. Emergency device. Internet of Things (IoT). Maria da Penha Law. Hardware prototyping.

SUMÁRIO

1 INTRODUÇÃO	9
2 FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS	10
2.1 Violência doméstica contra a mulher: conceitos e tipologias	10
2.2 Cenário brasileiro e indicadores de letalidade	10
2.3 Botão do Pânico como política pública complementar	11
2.4 Trabalhos correlatos	11
3 METODOLOGIA	12
3.1 Protocolo de validação adotado	12
4 ARQUITETURA DO DISPOSITIVO	13
4.1 Requisitos	13
4.2 Visão geral da arquitetura	14
4.3 Camada de hardware e firmware	14
4.4 Camada de comunicação e backend	14
4.5 Segurança, privacidade e adequação à LGPD	15
4.6 Camada de apresentação	17
5 PROTOTIPAGEM	17
5.1 Hardware utilizado	17
5.2 Pilha de software	18
5.3 Pipeline de eventos e desafios técnicos	19
5.4 Validação funcional	19
6 MODELO DE DISTRIBUIÇÃO	20
6.1 Justificativa e premissas	20
6.2 Atores e regras de negócio	21
6.3 Fluxo operacional	21
6.4 Custos e escalabilidade	22
6.5 Interoperabilidade com sistemas policiais existentes	22
7 RESULTADOS ESPERADOS	22
7.1 Comparação qualitativa com soluções existentes	23
7.2 Limitações e ressalvas	23
8 CONSIDERAÇÕES FINAIS	24
REFERÊNCIAS	26

Desenvolvimento de dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica: arquitetura, prototipagem e modelo de distribuição.

Title: Development of a discreet emergency activation device for women experiencing domestic violence: architecture, prototyping, and distribution model.

Guilherme Henrique Costa Vieira¹, Janio Rosa da Silva¹

¹Instituto Federal de Educação, Ciência e Tecnologia de Minas Gerais (IFMG)
Ouro Branco – MG – Brasil

guilhermehcvieira@hotmail.com, janio.rosa@ifmg.edu.br

Abstract. Introduction: Domestic violence against women remains a structural problem in Brazil, with femicide rates rising despite the legal framework provided by the Maria da Penha Law. Existing emergency response tools, such as the Panic Button, present operational limitations regarding discretion, autonomy, and coverage that restrict their effectiveness in cohabitation scenarios. **Objective:** This work proposes the development of a discreet emergency activation device for women experiencing domestic violence, integrating hardware architecture, functional prototyping, and a distribution model articulated with the protection network. **Methodology or Steps:** The methodology comprises a literature review on violence against women and existing protection technologies, the specification of functional and non-functional requirements, the design of the device's hardware/software architecture, the construction of a functional prototype, and the proposition of a distribution model integrated with specialized police stations (DEAMs) and reference centers (CRAMs). **Expected Results:** It is expected that the proposed device will overcome the discretion and coverage limitations of current solutions, providing a viable, low-cost, and scalable alternative for the rapid emergency triggering by women in situations of domestic violence, contributing to public protection policies.

Keywords Domestic violence, Emergency device, IoT, Maria da Penha Law, Hardware prototyping.

Resumo. Introdução: A violência doméstica contra a mulher persiste como problema estrutural no Brasil, com índices de feminicídio em ascensão mesmo diante do arcabouço jurídico instituído pela Lei Maria da Penha. As ferramentas atuais de resposta emergencial, como o Botão do Pânico, apresentam limitações operacionais quanto à discricção, autonomia e cobertura, que comprometem sua efetividade em cenários de coabitação com o agressor. **Objetivo:** Este trabalho propõe o desenvolvimento de um dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica, integrando arquitetura de hardware, prototipagem funcional e um modelo de distribuição articulado com a rede de proteção. **Metodologia ou Etapas:** A metodologia compreende a revisão bibliográfica sobre violência contra a

*mulher e tecnologias de proteção existentes, o levantamento de requisitos funcionais e não funcionais, o projeto da arquitetura de hardware e software do dispositivo, a construção de um protótipo funcional e a proposição de um modelo de distribuição integrado às delegacias especializadas (DEAMs) e aos centros de referência (CRAMs). **Resultados Esperados:** Espera-se que o dispositivo proposto supere as limitações de descrição e cobertura das soluções atuais, oferecendo uma alternativa viável, de baixo custo e escalável para o acionamento emergencial rápido por mulheres em situação de violência doméstica, contribuindo com as políticas públicas de proteção.*

Palavras-Chave Violência doméstica, Dispositivo de emergência, IoT, Lei Maria da Penha, Prototipagem de hardware.

1. Introdução

A violência doméstica e familiar contra a mulher constitui uma grave violação dos direitos humanos e um problema social estrutural no Brasil, com raízes históricas profundas e impacto cotidiano sobre milhões de vítimas [dos Santos e Cordeiro 2023, da Conceição da Silva Lima e Rodrigues 2022]. Apesar da promulgação da Lei nº 11.340/2006 (Lei Maria da Penha) e da tipificação do feminicídio pela Lei nº 13.104/2015, os indicadores de letalidade de gênero seguem em trajetória ascendente: somente em 2025, foram registradas 1.568 vítimas de feminicídio no país, crescimento de 4,7% em relação ao ano anterior, totalizando ao menos 13.703 mulheres assassinadas em razão de sua condição feminina desde a tipificação do crime [Fórum Brasileiro de Segurança Pública 2026].

Embora o arcabouço normativo brasileiro de proteção à mulher seja considerado avançado, a literatura jurídica e psicossocial aponta lacunas significativas na efetividade das políticas públicas de prevenção, especialmente no que se refere à capacidade de resposta rápida em situações de risco iminente [dos Santos e Cordeiro 2023]. As barreiras enfrentadas pelas vítimas no acesso aos serviços de apoio — agravadas por fatores interseccionais de raça, classe e gênero — comprometem a efetivação das medidas protetivas e perpetuam o ciclo de violência [da Conceição da Silva Lima e Rodrigues 2022].

Nesse contexto, dispositivos tecnológicos de acionamento emergencial, como o Botão do Pânico, foram incorporados às políticas públicas como instrumento de proteção complementar às medidas judiciais. Estudos sobre o perfil das mulheres usuárias desses dispositivos demonstram a relevância da iniciativa, mas também evidenciam limitações operacionais relevantes: dependência de equipamentos volumosos, baixa descrição em situações de coabitação com o agressor, restrição geográfica de cobertura e ausência de sistematização robusta dos dados de uso [Diatchuk e Schuartz 2023]. Tais limitações reduzem o alcance da medida e, em muitos casos, inviabilizam o acionamento justamente nas situações em que a vítima se encontra sob vigilância direta do agressor.

Diante desse cenário, este trabalho propõe o desenvolvimento de um dispositivo discreto de acionamento de emergência voltado para mulheres em situação de violência doméstica, contemplando três frentes integradas: (i) a definição da arquitetura de hardware e software, com foco em descrição, autonomia energética e confiabilidade na transmissão do sinal de emergência; (ii) a prototipagem funcional, validando a viabilidade

técnica da solução em cenários representativos de uso; e (iii) a proposição de um modelo de distribuição articulado com os órgãos da rede de proteção, de modo a viabilizar o acesso ao dispositivo pelas vítimas atendidas por delegacias especializadas (DEAMs) e centros de referência (CRAMs).

O presente artigo está organizado da seguinte forma. A Seção 2 apresenta a fundamentação teórica e os trabalhos correlatos. A Seção 3 descreve a metodologia de desenvolvimento. A Seção 4 detalha a arquitetura proposta para o dispositivo. A Seção 5 apresenta o processo de prototipagem. A Seção 6 discute o modelo de distribuição articulado com a rede de proteção. Por fim, a Seção 7 apresenta os resultados esperados e a Seção 8 traz as considerações finais e os apontamentos para trabalhos futuros.

2. Fundamentação Teórica e Trabalhos Correlatos

2.1. Violência Doméstica contra a Mulher: conceitos e tipologias

A violência contra a mulher é compreendida como um fenômeno social estrutural, com raízes históricas profundas, que se manifesta em múltiplas dimensões — física, psicológica, sexual, patrimonial e moral [dos Santos e Cordeiro 2023]. Diferentemente dos crimes comuns, a violência doméstica e familiar caracteriza-se pela habitualidade, pela existência de relações afetivas entre vítima e agressor e, sobretudo, pela hierarquia de gênero que sustenta o ato violento [dos Santos e Cordeiro 2023]. Lima e Rodrigues [da Conceição da Silva Lima e Rodrigues 2022] destacam, ainda, a necessidade de uma leitura interseccional do fenômeno, na qual marcadores de raça, classe e gênero atuam de forma indissociável e interdependente, ampliando as opressões vivenciadas pelas vítimas e dificultando seu rompimento com o ciclo de violência.

2.2. Cenário brasileiro e indicadores de letalidade

No Brasil, a Lei nº 11.340/2006 (Lei Maria da Penha) representou um marco no enfrentamento à violência doméstica, ao estabelecer mecanismos para prevenir, coibir e erradicar a prática [dos Santos e Cordeiro 2023]. Entretanto, mais de uma década após sua promulgação, os indicadores seguem alarmantes. Segundo o Fórum Brasileiro de Segurança Pública [Fórum Brasileiro de Segurança Pública 2026], somente em 2025 foram registradas 1.568 vítimas de feminicídio no país, representando um crescimento de 4,7% em relação ao ano anterior. Desde a tipificação do crime de feminicídio pela Lei nº 13.104/2015, ao menos 13.703 mulheres foram assassinadas em razão de sua condição feminina, com a maioria dos casos decorrendo de agressão de parceiros íntimos no contexto doméstico [Fórum Brasileiro de Segurança Pública 2026].

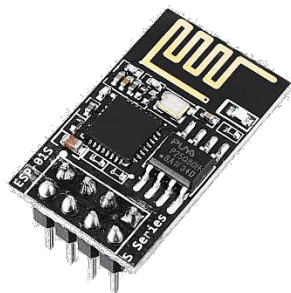
A persistência desses números evidencia limitações na efetividade das políticas públicas de proteção. Santos e Cordeiro [dos Santos e Cordeiro 2023] apontam que, embora existam instituições e órgãos especializados — como as Delegacias Especializadas de Atendimento à Mulher (DEAMs) e os Centros de Referência de Atendimento à Mulher (CRAMs) —, persistem barreiras significativas no acesso e na efetividade das medidas. Os Centros de Referência tendem a apresentar atuação mais eficiente em razão do caráter multidisciplinar do atendimento, enquanto as DEAMs, ainda que importantes, esbarram em limitações de cobertura, horário de funcionamento e capacitação [dos Santos e Cordeiro 2023].

2.3. Botão do Pânico como política pública complementar

Como resposta à demanda por respostas rápidas em situações de risco iminente, diversos municípios brasileiros adotaram dispositivos de acionamento emergencial — popularmente conhecidos como Botão do Pânico — articulados às medidas protetivas de urgência da Lei Maria da Penha. Diatchuk e Schuartz [Diatchuk e Schuartz 2023] sistematizaram dados sobre o perfil de mulheres usuárias do dispositivo em um município do litoral paranaense e demonstraram a relevância da iniciativa, mas também apontaram limitações: ausência de sistematização robusta dos dados, dependência operacional de equipamentos com forma-fator pouco discreto e cobertura geográfica restrita à área de patrulhamento conveniada.

Tais limitações são particularmente críticas em cenários de coabitação com o agressor, em que o acionamento de um dispositivo visualmente identificável pode escalar a violência ao invés de mitigá-la. Além disso, a ausência de integração entre o dispositivo, os contatos pessoais da vítima e a rede de proteção reduz a eficácia da resposta, deixando o acionamento dependente exclusivamente da chegada de uma viatura policial.

A Figura 1 ilustra essa diferença de forma-fator. À esquerda, o módulo ESP-01 (cerca de 25×15 mm) adotado neste trabalho; à direita, o botão de pânico atualmente acoplado a tornozeleiras eletrônicas no contexto de monitoramento eletrônico previsto pela Lei Maria da Penha. Embora a solução institucional vigente já represente um avanço em portabilidade frente aos modelos anteriores, o dispositivo permanece visualmente identificável e demanda um aparato adicional, o que compromete a discrição em situações de coabitação. Em contraste, o módulo embarcado proposto neste trabalho permite encapsulamento em objetos de uso pessoal cotidiano, tornando o acionamento praticamente imperceptível.



(a) ESP-01 (proposta deste trabalho).



(b) Tornozeleira eletrônica com botão de pânico acoplado, utilizada em programas oficiais de monitoramento (fonte: TJMG).

Figura 1. Comparativo de forma-fator entre o módulo embarcado proposto (a) e a solução institucional vigente (b). Embora pequena, a tornozeleira é visualmente identificável e dificilmente discreta em cenários de coabitação com o agressor.

2.4. Trabalhos correlatos

Soluções baseadas em Internet das Coisas (IoT) para segurança pessoal têm sido exploradas tanto no meio acadêmico quanto em produtos comerciais, geralmente

envolvendo wearables com botão físico, aplicativos móveis de denúncia e plataformas integradas de despacho. Contudo, a maior parte das soluções comerciais é proprietária, de custo elevado e desenhada para usos genéricos, não considerando os requisitos específicos do contexto de violência doméstica — em especial a necessidade de discrição extrema, baixo custo unitário (para viabilizar distribuição em larga escala pelo poder público) e integração com a rede de proteção institucional. Esta é a lacuna que o presente trabalho busca endereçar.

3. Metodologia

Este trabalho caracteriza-se como uma pesquisa aplicada, de natureza exploratória e descritiva, conduzida sob o paradigma de prototipagem funcional em sistemas embarcados. A abordagem é predominantemente *descritivo-técnica*, centrada na concepção, integração e verificação operacional de um protótipo em ambiente controlado, e não constitui um experimento estatístico-inferencial — opção deliberada e coerente com o estágio de validação conceitual em que se encontra o sistema. Os indicadores de desempenho reportados ao longo do texto (em especial na Seção 5) têm caráter *indicativo* e foram coletados em condições laboratoriais; uma validação empírica em contexto operacional real — com tamanho amostral planejado, delineamento estatístico, análise inferencial e protocolos padronizados — é apresentada como agenda explícita de trabalhos futuros (Seção 8). O desenvolvimento foi organizado em cinco etapas sequenciais e iterativas:

- (i) **Revisão bibliográfica:** levantamento da literatura sobre violência doméstica, políticas públicas de proteção à mulher e tecnologias correlatas, com base em artigos científicos, legislação vigente e relatórios institucionais [dos Santos e Cordeiro 2023, da Conceição da Silva Lima e Rodrigues 2022, Diatchuk e Schuartz 2023, Fórum Brasileiro de Segurança Pública 2026];
- (ii) **Levantamento de requisitos:** definição de requisitos funcionais e não funcionais a partir das limitações operacionais identificadas nas soluções existentes [Diatchuk e Schuartz 2023], com ênfase em discrição, baixo custo, autonomia energética e integração com a rede de proteção;
- (iii) **Projeto da arquitetura:** especificação do dispositivo de hardware (microcontrolador, módulo de comunicação, gatilho discreto) e da plataforma de software (servidor de aplicação, broker de mensagens, painel de despacho e portal do usuário);
- (iv) **Prototipagem funcional:** implementação do firmware embarcado, do servidor backend, do painel operacional para a polícia e do portal de cadastro do usuário, com validação por testes funcionais em ambiente controlado;
- (v) **Proposição do modelo de distribuição:** definição do fluxo de cadastro, entrega, acionamento, despacho e devolução do dispositivo, articulado com as DEAMs, CRAMs e equipes de patrulhamento, à luz das diretrizes da Lei Maria da Penha e das boas práticas observadas em municípios que já operam serviços similares [dos Santos e Cordeiro 2023, Diatchuk e Schuartz 2023].

3.1. Protocolo de validação adotado

A etapa de prototipagem funcional foi conduzida segundo um protocolo interno reprodutível, descrito a seguir e instanciado quantitativamente na Seção 5:

- **Critérios de aceitação:** cada RF e RNF da Seção 4 foi associado a um cenário de teste correspondente, considerando-se atendido quando o fluxo observado convergiu para o resultado esperado dentro dos limites aceitáveis para um sistema de emergência;
- **Métricas instrumentadas:** latência fim-a-fim do acionamento (clique no botão até a exibição no painel via WebSocket), latência de notificação Telegram, tempo de reconexão após queda de Wi-Fi, sucesso de entrega de mensagens MQTT e correção do despacho georreferenciado;
- **Tamanho amostral exploratório:** dezenas de ciclos de acionamento por cenário, suficientes para caracterizar tendência, mas reconhecidamente insuficientes para inferência estatística — limitação assumida e endereçada como trabalho futuro;
- **Ambiente:** rede Wi-Fi 2,4 GHz doméstica com um único *access point*, broker MQTT e backend executando em contêineres Docker na mesma rede do dispositivo, cliente policial em navegador na mesma sub-rede;
- **Reprodutibilidade:** o código-fonte, o `docker-compose.yml` e as instruções de *bootstrap* permanecem versionados em repositório próprio, permitindo que terceiros reexecutem os mesmos cenários e estendam o protocolo para os contextos elencados na Seção 8 (ambientes urbanos reais, regiões com conectividade instável, cenários com múltiplos roteadores ou interferência de RF e quedas prolongadas de energia/Internet).

A escolha por um protocolo descritivo, e não experimental no sentido estrito, é consciente: o estado atual do trabalho corresponde a uma *validação conceitual e técnica*, condição usual em projetos de prototipagem exploratória em sistemas embarcados [Diatchuk e Schuartz 2023]. A transição para um estudo experimental com delineamento estatístico depende de pré-condições externas — aprovação em comitê de ética, parceria institucional com DEAM/CRAM ou polícia militar, recrutamento de operadores e (eventualmente) de usuárias —, sendo projetada como etapa subsequente e detalhada na Seção 8.

4. Arquitetura do Dispositivo

4.1. Requisitos

A partir da fundamentação teórica e da análise das limitações apontadas em [Diatchuk e Schuartz 2023], foram especificados os seguintes requisitos:

Requisitos funcionais (RF):

- **RF01:** O dispositivo deve permitir o acionamento de três níveis distintos de alerta (*risco*, *risco muito sério*, *risco de morte*), correspondentes a diferentes padrões de pressão sobre o gatilho;
- **RF02:** O sistema deve transmitir o alerta em tempo real para um painel de despacho operado por agentes de segurança pública;
- **RF03:** O sistema deve notificar contatos pessoais previamente cadastrados pela vítima, simultaneamente ao acionamento;
- **RF04:** O sistema deve registrar localização da vítima (cadastrada e/ou em tempo real) associada ao alerta, viabilizando o despacho georreferenciado;
- **RF05:** O dispositivo deve operar via rede sem fio convencional, dispensando infraestrutura específica;

- **RF06:** O sistema deve suportar múltiplas zonas de atuação policial, roteando os alertas para a viatura mais próxima.

Requisitos não funcionais (RNF):

- **RNF01 (Discrição):** o dispositivo deve ter forma-fator pequeno e camuflável em objetos de uso pessoal, atendendo às necessidades de coabitação com o agressor [Diatchuk e Schuartz 2023];
- **RNF02 (Baixo custo):** o custo unitário deve viabilizar a distribuição em larga escala pelo poder público;
- **RNF03 (Confiabilidade):** a entrega do alerta deve ser garantida mesmo diante de falhas momentâneas de conectividade;
- **RNF04 (Privacidade):** dados pessoais sensíveis devem ser protegidos por autenticação e armazenamento seguro;
- **RNF05 (Integração):** o sistema deve oferecer interface clara de despacho operacional para as polícias militares e civis.

4.2. Visão geral da arquitetura

A solução é organizada em quatro componentes principais: (i) o *dispositivo embarcado*, baseado no microcontrolador ESP-01 (ESP8266), responsável por capturar o acionamento físico e publicar o alerta; (ii) um *broker MQTT* (Eclipse Mosquitto), que recebe e distribui as mensagens; (iii) um *servidor de aplicação* construído em Python com FastAPI, responsável por persistir os alertas, enriquecê-los com dados georreferenciados, propagar eventos via WebSocket e notificar contatos pessoais; e (iv) duas *interfaces web*: o portal do usuário e o painel de despacho da polícia.

4.3. Camada de hardware e firmware

O dispositivo embarcado utiliza o módulo ESP-01 com 1MB de *flash* (board `esp01_1m`), escolhido por seu baixo custo unitário, capacidade de comunicação Wi-Fi nativa e ampla disponibilidade no mercado nacional. O firmware foi desenvolvido em C++ sobre o framework `arduino-esp8266`, com o gerenciamento de pacotes feito via PlatformIO.

O dispositivo armazena na EEPROM apenas as credenciais Wi-Fi e um identificador único (UUID), de modo que dados pessoais sensíveis (nome, endereço e telefone) ficam centralizados no servidor e podem ser atualizados sem necessidade de reconfiguração do hardware. No primeiro uso, o ESP sobe um ponto de acesso temporário (PANICO-SETUP) com portal cativo em `192.168.4.1`, no qual o usuário informa as credenciais da rede doméstica. A partir desse momento, o dispositivo conecta-se ao broker MQTT via Wi-Fi e fica em estado de prontidão.

A interpretação do gatilho é realizada localmente pelo firmware, com filtragem por *debounce* (50 ms) e identificação dos três níveis de alerta com base em padrões temporais distintos: pressão de 1 a 3 segundos (RISCO), pressão acima de 3 segundos (RISCO_MUITO_SERIO) e três cliques rápidos dentro de uma janela de 2 segundos (RISCO_DE_MORTE). Um período de *cooldown* de 5 segundos previne disparos duplicados.

4.4. Camada de comunicação e backend

A comunicação dispositivo-servidor adota o protocolo MQTT, leve e adequado para cenários IoT com restrição de banda. Três tópicos compõem o contrato de mensagens:

- `panico/alerta` — dispositivo → servidor, contendo *payload* JSON com UUID e nível de alerta;
- `panico/status/<device_uuid>` — dispositivo → servidor, mensagens *online/offline* com *Last Will and Testament*;
- `panico/ack/<device_uuid>` — servidor → dispositivo, confirmação de recebimento.

O servidor backend, escrito em Python com FastAPI e SQLAlchemy 2.x (PostgreSQL), expõe duas rotas de ingresso de alertas: a rota MQTT (caminho de produção) e uma rota HTTP POST `/api/alertas/` (utilizada para integração e testes). Ambos os caminhos convergem para o mesmo registro persistido na base, garantindo um histórico unificado.

Ao receber um alerta, o servidor: (a) localiza o dispositivo por seu UUID e recupera o usuário associado; (b) faz um *snapshot* dos dados pessoais e da localização da vítima na linha do alerta — preservando a estabilidade do histórico mesmo que o perfil seja editado posteriormente; (c) aciona o módulo de *zone routing* (consulta espacial *point-in-polygon* sobre as zonas policiais cadastradas) para taggear o alerta com a zona correta; (d) propaga o evento via WebSocket para o painel de despacho da polícia daquela zona; e (e) dispara notificações via Telegram para os contatos pessoais cadastrados.

A precedência de localização adota a seguinte regra: coordenadas presentes no *payload* têm prioridade; na ausência destas, utiliza-se a localização *live* do usuário (capturada pelo navegador quando ele está logado no portal e considerada válida por até 10 minutos); como último recurso, recorre-se ao endereço cadastrado, geocodificado via Nominatim/OpenStreetMap.

A Figura 2 apresenta o diagrama de sequência da lógica completa da aplicação, desde o acionamento físico do botão pela vítima até a confirmação do recebimento (*ack*) recebida pelo dispositivo, evidenciando a interação entre os atores e componentes do sistema.

4.5. Segurança, privacidade e adequação à LGPD

Por lidar com dados pessoais — e, em parte, com dados pessoais sensíveis — de mulheres em situação de violência (nome, endereço, contatos, localização e histórico de alertas), o sistema está sujeito à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados, LGPD) [dos Santos e Cordeiro 2023]. A plataforma foi concebida segundo princípios de *privacy by design*, com as seguintes medidas:

- **Minimização de dados:** o dispositivo embarcado armazena exclusivamente as credenciais Wi-Fi e o UUID — nenhum dado pessoal trafega ou repousa no hardware, reduzindo o risco em caso de extravio ou apreensão;
- **Finalidade específica:** os dados são tratados unicamente para viabilizar o acionamento emergencial, o despacho policial e a notificação dos contatos cadastrados, em consonância com o princípio da finalidade (LGPD, art. 6º, I);
- **Segurança em repouso e em trânsito:** senhas com *hash bcrypt*, autenticação por JWT (HS256) para as interfaces administrativas e operacionais, e previsão de TLS no transporte HTTP/WebSocket e TLS sobre MQTT em implantação de produção;

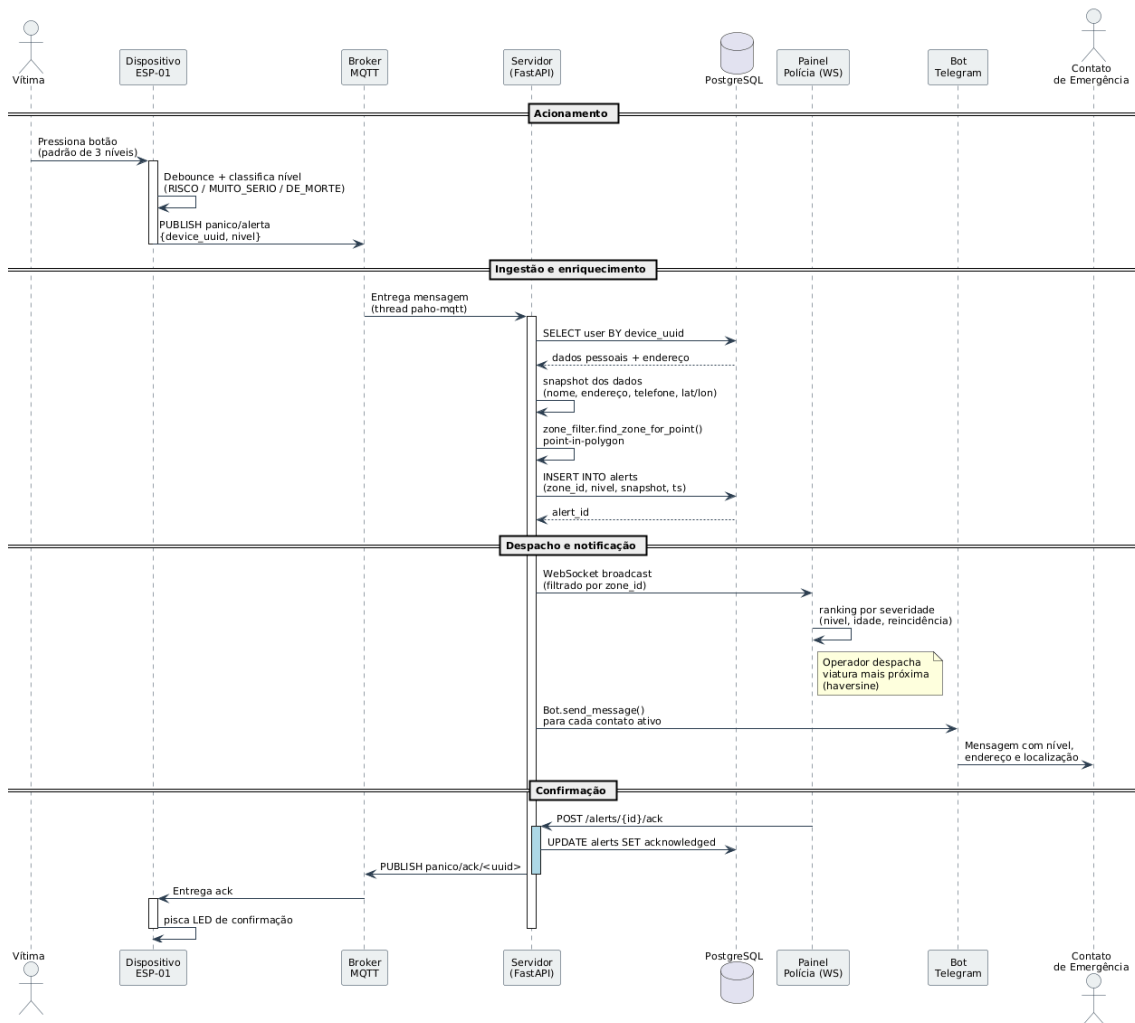


Figura 2. Diagrama de sequência da lógica da aplicação: do acionamento físico ao despacho operacional e à notificação dos contatos de emergência.

- **Snapshot do alerta para rastreabilidade jurídica:** os dados pessoais e a localização da vítima são copiados para o registro do alerta no momento da ingestão, impedindo que edições posteriores no perfil distorçam o histórico;
- **Compartimentalização de acesso:** contatos de emergência não possuem conta no sistema — recebem apenas as mensagens via Telegram após confirmação do *token*, reduzindo a superfície de exposição de dados;
- **Governança institucional:** prevê-se que a entidade pública responsável pela operação (DEAM, CRAM ou secretaria de segurança) designe um encarregado pelo tratamento de dados (DPO) e mantenha o registro das operações de tratamento, conforme o art. 41 da LGPD.

Limitação conhecida e plano de mitigação para a ingestão de alertas. As rotas de ingresso de alertas (MQTT e HTTP) operam, no protótipo atual, sem autenticação forte: o emissor é identificado exclusivamente pelo UUID do dispositivo. Esse desenho privilegia simplicidade e baixa latência no contexto laboratorial, mas abre margem, em uma implantação real, a *spoofing* de UUID e injeção de falsos alertas. Para uma versão de produção, propõem-se três camadas complementares de mitigação, compatíveis com a

arquitetura vigente: (a) **autenticação mútua TLS (mTLS)** com certificado provisionado por dispositivo durante o cadastro institucional pela DEAM/CRAM; (b) **assinatura HMAC do *payload*** com chave derivada do UUID e de um *secret* compartilhado, rotacionável a cada (re)cadastro; e (c) **ACLs no broker MQTT**, restringindo cada cliente publicador aos tópicos vinculados ao seu próprio UUID. Tais medidas inviabilizam a injeção de falsos alertas por terceiros sem custo adicional significativo de latência, e seu projeto detalhado integra a agenda de trabalhos futuros descrita na Seção 8.

4.6. Camada de apresentação

Duas interfaces web complementares atendem aos perfis de usuário do sistema:

- **Portal do usuário** (`static/portal.html`): permite à mulher cadastrar seus dados pessoais, vincular o dispositivo, gerenciar contatos de emergência e enviar localização em tempo real (*push* de GPS a cada 60 segundos enquanto a sessão estiver ativa);
- **Painel de despacho policial** (`frontend/`): *Single-Page Application* React 18 + TypeScript + Vite + Tailwind + react-leaflet, com autenticação JWT específica para policiais e operadores. O painel exibe os alertas filtrados por zona, classifica-os por uma fórmula de severidade que combina nível de alerta, idade do alerta e reincidência da vítima, e oferece o despacho da viatura mais próxima por distância haversiana.

A vinculação dos contatos de emergência ao Telegram ocorre em duas etapas: o sistema gera um *token* de 8 caracteres com validade de 7 dias para cada contato cadastrado; a vítima compartilha o *token* com o contato, que envia o comando `/start <token>` ao bot, registrando seu `chat_id` no servidor. A partir daí, todas as mensagens de alerta são enviadas automaticamente.

5. Prototipagem

5.1. Hardware utilizado

A montagem do protótipo utilizou os seguintes componentes:

- Módulo Wi-Fi ESP-01 (ESP8266) com 1 MB de *flash*;
- Bateria de íon-lítio recarregável de 500 mAh (3,7 V), com circuito de proteção integrado contra sobrecarga, sobredescarga e curto-circuito;
- Conversor *step-up*/regulador 3,3 V de baixo *quiescent current*, alimentando o ESP-01 a partir da bateria;
- Botão tátil miniatura normalmente aberto, conectado ao GPIO0 com *pull-up* interno (acionamento por aterramento);
- LED SMD indicador de status conectado ao GPIO2 (ativo em nível baixo, com resistor limitador de 220 Ω);
- Adaptador USB-Serial CH340 ou CP2102 (utilizado apenas em bancada para a gravação do firmware);
- Roteador Wi-Fi doméstico para conexão com a Internet.

Justificativa do dimensionamento físico e energético

O conjunto eletrônico foi dimensionado deliberadamente para ocupar o menor volume possível. O módulo ESP-01 mede aproximadamente 25×15 mm; a bateria de 500 mAh adotada possui formato *slim* (pouch *LiPo*) com espessura inferior a 5 mm e área da ordem de 30×20 mm; o botão tátil e o LED SMD ocupam frações de centímetro. Somados ao regulador e ao circuito de proteção, o conjunto integral cabe em um volume da ordem de poucos centímetros cúbicos — compatível com o interior de objetos cotidianos de uso feminino.

Esse dimensionamento atende simultaneamente ao **RNF01 (discrição)** e ao **RNF02 (baixo custo)**: o conjunto pode ser encapsulado em *cases* que se confundem com itens triviais do dia a dia da vítima — *e.g.*, embalagens de protetor labial, tubos de batom, frascos de hidratante de bolso, chaveiros, pingentes, broches, capas de celular, enfeites de cabelo, entre outros. A escolha do encapsulamento é, ela própria, parte da estratégia de proteção: o dispositivo não deve parecer um dispositivo. Ao confundir-se com objetos pessoais comuns, evita-se o efeito contrário ao desejado — observado nas soluções institucionais vigentes, em que o forma-fator visualmente identificável do botão de pânico pode escalar a violência ao sinalizar ao agressor que a vítima está, naquele momento, denunciando-o (Figura 1).

A eficiência energética foi tratada como restrição de projeto, não como otimização secundária. Nos modos de operação típicos do firmware:

- Em *idle* com Wi-Fi conectado, o ESP-01 consome aproximadamente 70–80 mA em média, com picos durante a transmissão de pacotes;
- Em modo *modem-sleep* (Wi-Fi suspenso entre *keep-alives* MQTT), o consumo cai para a faixa de 15–20 mA;
- Em modo *light-sleep*, com despertar por *interrupt* no GPIO0 (botão), o consumo médio cai para a casa de poucos miliamperes.

Adotando uma estratégia de *light-sleep* entre *heartbeats* MQTT periódicos, o protótipo projeta autonomia da ordem de dezenas de horas a poucos dias com a bateria de 500 mAh, dependendo do intervalo de *keep-alive* escolhido. Esse balanço é deliberado: privilegia-se uma bateria pequena, recarregável por porta micro-USB ou cabo magnético embutido na carcaça, em detrimento de uma bateria maior porém visualmente intrusiva. A vítima recarrega o dispositivo nos mesmos contextos em que recarregaria um carregador portátil ou um *smartwatch*, sem chamar atenção.

A escolha do ESP-01 atende, adicionalmente, ao **RNF02 (baixo custo)**: seu preço unitário no varejo nacional é da ordem de R\$ 15–25, e a bateria de 500 mAh acresce algo entre R\$ 10–20 ao custo de materiais — mantendo o conjunto dentro da faixa que viabiliza distribuição em larga escala pelo poder público.

5.2. Pilha de software

A implementação do servidor adotou as seguintes tecnologias:

- **FastAPI** — *framework* web Python com suporte nativo a operações assíncronas e geração automática de documentação OpenAPI;

- **SQLAlchemy 2.x + Alembic** — ORM e gerenciamento de migrações sobre PostgreSQL;
- **Eclipse Mosquitto** — broker MQTT com suporte a QoS e *Last Will*;
- **paho-mqtt** — cliente MQTT Python utilizado pelo servidor para se inscrever nos tópicos de alerta e status;
- **python-telegram-bot** — biblioteca para envio das notificações aos contatos de emergência;
- **python-jose + bcrypt** — autenticação JWT (HS256) e *hash* de senhas;
- **Docker Compose** — orquestração dos serviços (*Postgres*, *Mosquitto* e API) em ambiente isolado;
- **React 18 + TypeScript + Vite + Tailwind CSS + react-leaflet** — Single-Page Application do painel de despacho policial.

5.3. Pipeline de eventos e desafios técnicos

Um aspecto crítico da implementação envolveu a integração entre o cliente MQTT — que executa em *thread* dedicada via `loop_forever` do *paho-mqtt* — e o *event loop* assíncrono do FastAPI, responsável pela difusão dos alertas via WebSocket. Como a rotina `await manager.broadcast(...)` não pode ser invocada diretamente da *thread* MQTT, adotou-se o padrão `asyncio.run_coroutine_threadsafe`, com captura de uma referência ao *loop* principal durante a inicialização da aplicação. Esse desenho preserva a integridade do modelo de concorrência e evita corrida em estruturas internas do FastAPI.

Para o despacho operacional, foi implementado o roteamento por zonas geográficas: cada zona é representada por um polígono persistido na base e cada usuário policial pode estar associado a uma zona específica. O servidor executa, no momento da ingestão do alerta, uma consulta espacial *point-in-polygon* para identificar a zona correspondente; em seguida, a difusão WebSocket é restrita aos operadores daquela zona, com supervisores recebendo todos os eventos.

5.4. Validação funcional

Foram realizados testes funcionais em ambiente controlado, organizados em cenários numerados e vinculados aos requisitos da Seção 4. O ambiente consistiu em rede Wi-Fi 2,4 GHz doméstica, com broker MQTT e backend executando em contêineres Docker na mesma rede do dispositivo e cliente policial em navegador na mesma sub-rede:

- **C1 — Acionamento e classificação de nível (RF01)**: ciclos repetidos para cada um dos três padrões temporais (RISCO, RISCO_MUITO_SERIO e RISCO_DE_MORTE), avaliando a correta interpretação pelo firmware após *debounce*;
- **C2 — Latência fim-a-fim (RF02)**: tempo decorrido entre o evento de clique no botão e a exibição do alerta no painel via WebSocket;
- **C3 — Resiliência a queda de Wi-Fi (RNF03)**: desligamento momentâneo do *access point* (na ordem de segundos a dezenas de segundos), avaliando a reconexão automática do ESP-01 e a entrega de alertas *enfileirados* no firmware;
- **C4 — Concorrência (RF02, RF06)**: múltiplos dispositivos virtuais publicando alertas simultâneos no broker, avaliando o roteamento por zona;

- **C5 — Notificação aos contatos (RF03):** ciclo completo de cadastro de contato, geração e validação do *token*, envio de `/start` ao bot e recepção da mensagem após o disparo;
- **C6 — Despacho georreferenciado (RF04, RF06):** validação da seleção da viatura mais próxima por distância haversiana, com posições de viatura simuladas via API administrativa.

A Tabela 1 consolida os indicadores observados em ambiente controlado. **Importante:** os valores têm caráter *indicativo* e *exploratório*, refletindo dezenas de ciclos por cenário em um único ambiente — **não constituem *benchmark* estatístico nem caracterização formal de desempenho em produção**. Conforme reconhecido na Seção 3, não foram avaliados neste estágio: ambientes com múltiplos *access points* e *roaming*, redes congestionadas (próximas a aglomerações, shoppings ou subestações), conectividade celular/móvel, zonas rurais com cobertura intermitente, quedas prolongadas de energia, jitter sustentado, cenários adversariais de injeção de tráfego e indicadores formais como MTBF, disponibilidade longitudinal e taxa de perda sob *stress*. A caracterização desses regimes é endereçada na Seção 8 como agenda de trabalho futuro.

Tabela 1. Indicadores funcionais observados em ambiente controlado (n exploratório; valores indicativos, não inferenciais).

Cenário	Indicador	Observação típica
C1	Acerto na classificação de nível	100% nos ciclos executados
C2	Latência fim-a-fim (clique → painel)	Sub-segundo na rede local
C3	Tempo de reconexão Wi-Fi	Poucos segundos após retorno do AP
C3	Alertas perdidos na queda momentânea	Nenhum (com QoS apropriado no MQTT)
C4	Ordem de chegada em concorrência	Sem perda observada
C5	Recepção da notificação Telegram	Poucos segundos após o alerta
C6	Seleção da viatura mais próxima	Coerente em todos os ciclos

A validação atual atende ao propósito de demonstrar a *viabilidade funcional* do protótipo e a aderência aos requisitos da Seção 4, mas não substitui um estudo experimental formal — o que é discutido em maior detalhe na Seção 7 e formalizado como trabalho futuro na Seção 8.

6. Modelo de Distribuição

6.1. Justificativa e premissas

A literatura mostra que o sucesso de iniciativas como o Botão do Pânico depende menos do dispositivo isolado e mais de sua articulação institucional com a rede de proteção [Diatchuk e Schuartz 2023, dos Santos e Cordeiro 2023]. Tomando como premissa que a vítima já está em contato com uma DEAM ou um CRAM — locais usualmente referenciados por meio de medidas protetivas de urgência — o modelo proposto integra-se aos fluxos institucionais existentes, em vez de constituir um canal paralelo.

A distribuição é estruturada em torno de três princípios: (i) **discrição operacional**, com o dispositivo entregue em embalagem neutra e formatos que permitam camuflagem em objetos de uso cotidiano da vítima; (ii) **baixo custo unitário**, viabilizado pela escolha

do ESP-01 e pelo uso integral de software livre, eliminando custos de licenciamento; e (iii) **escalabilidade horizontal**, com o backend containerizado via Docker, capaz de servir dezenas a centenas de zonas operacionais sem mudança arquitetural.

6.2. Atores e regras de negócio

Quatro perfis de usuário compõem o sistema:

- **Vítima cadastrada:** mulher referenciada por DEAM, CRAM ou medida protetiva, que recebe o dispositivo e acessa o portal pessoal para gerenciar seu perfil, dispositivo vinculado e contatos de emergência;
- **Contato de emergência:** pessoa de confiança indicada pela vítima (familiar, amiga, vizinha), que recebe notificações via Telegram e não possui conta no sistema, garantindo que sua exposição se limite ao estritamente necessário;
- **Operador/policial:** agente público autenticado (JWT) com acesso ao painel de despacho, opcionalmente vinculado a uma zona policial específica;
- **Supervisor:** perfil sem zona vinculada, com visão global dos alertas e capacidade de redistribuição entre zonas.

As principais regras de negócio são: **(R1)** um dispositivo só pode estar vinculado a uma vítima por vez, mas pode ser realocado mediante reset no portal; **(R2)** os dados pessoais da vítima são copiados para o registro do alerta no momento da ingestão (*snapshot*), preservando a estabilidade do histórico para fins judiciais; **(R3)** os contatos de emergência só recebem o `chat_id` vinculado após a confirmação do *token* no bot, evitando exposição inadvertida; **(R4)** alertas são roteados automaticamente à zona policial cuja área contém as coordenadas no momento do disparo — supervisores recebem todos os eventos para fins de monitoramento; **(R5)** a fórmula de severidade priorizando o atendimento na fila considera nível do alerta, idade do alerta e reincidência (contagem de alertas dos últimos 30 dias da mesma vítima ou dispositivo); e **(R6)** os dados pessoais sensíveis estão protegidos por autenticação e criptografia (*bcrypt* para senhas, JWT HS256 para sessão), enquanto rotas de ingestão de alerta são intencionalmente desautenticadas para minimizar latência — confiando-se no UUID do dispositivo como mecanismo implícito de identificação.

6.3. Fluxo operacional

O ciclo de vida do dispositivo articula a rede de proteção da seguinte forma:

1. **Cadastro inicial:** a vítima é referenciada à equipe técnica (vinculada à DEAM ou CRAM) que opera o portal administrativo, cria seu perfil, vincula o dispositivo (gerando ou registrando o UUID) e orienta a configuração da rede Wi-Fi via portal cativo;
2. **Cadastro de contatos:** a vítima registra contatos de emergência no portal e compartilha os *tokens* de vinculação com cada um deles, fora da banda do sistema;
3. **Acionamento:** em situação de risco, a vítima pressiona o botão segundo o padrão correspondente ao nível desejado;
4. **Despacho e notificação:** o servidor identifica a zona, propaga o alerta ao painel da polícia daquela zona e dispara mensagens Telegram para os contatos cadastrados;
5. **Atendimento:** o operador despacha a viatura mais próxima (ranqueada por distância haversiana sobre as posições reportadas pelas viaturas), e o painel passa a acompanhar a evolução do atendimento até o fechamento do incidente;

6. **Devolução ou troca:** ao fim do período de medida protetiva, o dispositivo é devolvido à equipe responsável e pode ser reconicionado para outra vítima — preservando-se o histórico de alertas associado ao perfil original.

6.4. Custos e escalabilidade

O custo material por unidade situa-se em torno de R\$ 40–60, considerando o ESP-01, fonte/bateria, botão tátil, LED, encapsulamento e mão de obra de montagem. Esse valor é uma fração do custo de soluções comerciais equivalentes e viabiliza a aquisição em larga escala por convênios entre prefeituras, secretarias estaduais de segurança pública e o Ministério da Mulher. No lado do servidor, a arquitetura containerizada permite escalonamento horizontal: cada município ou estado pode operar uma instância independente, ou múltiplos municípios podem compartilhar uma única instância segmentada por zonas — modelo particularmente adequado para regiões metropolitanas e para municípios de menor porte que não dispõem de infraestrutura própria [dos Santos e Cordeiro 2023].

6.5. Interoperabilidade com sistemas policiais existentes

Para que a solução se integre à cadeia institucional de proteção sem constituir um canal paralelo, prevê-se a *interoperabilidade* do painel de despacho com sistemas policiais já consolidados — como o **Registro de Eventos de Defesa Social (REDS)**, utilizado em Minas Gerais, os sistemas estaduais de *Computer-Aided Dispatch* (CAD) das polícias militares e programas correlatos como o **SOS Mulher** operado em algumas unidades da federação (notadamente São Paulo). A arquitetura baseada em API REST e WebSocket facilita essa integração em duas direções: (i) *exportação* dos alertas para o sistema institucional vigente, registrando a ocorrência no fluxo oficial de boletim e preservando a cadeia de despacho da polícia militar; e (ii) *importação* de informações relevantes (posições de viaturas, status de ocorrências, histórico da vítima) para enriquecer a fórmula de severidade e qualificar o despacho.

Essa abordagem reforça o caráter incremental da proposta: somar-se à infraestrutura existente, em vez de substituí-la, reduz a fricção de adoção e aproveita o investimento público já realizado em sistemas como o REDS. O detalhamento técnico dessas integrações depende de acesso aos contratos de interoperabilidade institucionais e é endereçado como trabalho futuro (Seção 8).

7. Resultados Esperados

Os resultados parciais obtidos até o momento confirmam a viabilidade técnica da solução. O protótipo executa o ciclo completo de acionamento, transmissão MQTT, persistência, despacho via WebSocket e notificação Telegram. O painel de despacho policial em React apresenta os alertas em tempo real, ranqueados pela fórmula de severidade, e suporta o despacho georreferenciado de viaturas. O *deploy* via Docker Compose foi validado em ambiente local, e o código encontra-se modularizado em camadas (modelos, roteadores, serviços), favorecendo a manutenção e a evolução incremental.

A partir da arquitetura descrita e dos indicadores observados (Tabela 1), formulam-se três *hipóteses* de superioridade do dispositivo proposto frente às soluções tradicionais de Botão do Pânico, a serem confirmadas em testes futuros: (i) **discrição**, em

razão do forma-fator reduzido e da ausência de marcadores visuais explícitos; (ii) **escala de adoção**, viabilizada pelo baixo custo unitário e pela arquitetura de código aberto; e (iii) **tempo de resposta**, dada a integração direta com painéis operacionais e canais de notificação informais (contatos pessoais via Telegram), reduzindo a dependência exclusiva da chegada da viatura policial [Diatchuk e Schuartz 2023].

7.1. Comparação qualitativa com soluções existentes

A Tabela 2 sintetiza uma comparação *qualitativa* entre a proposta deste trabalho e duas referências em uso no Brasil: o botão de pânico acoplado a tornozeleira eletrônica em programas oficiais de monitoramento [Diatchuk e Schuartz 2023] e os botões de pânico municipais convencionais, distribuídos por convênios entre prefeituras e polícias militares. A comparação baseia-se em características arquiteturais e operacionais documentadas — **não em benchmarking empírico direto**, cuja realização demanda acesso aos equipamentos, contratos e protocolos institucionais e é endereçada como trabalho futuro (Seção 8).

Tabela 2. Comparação qualitativa entre a proposta e soluções existentes no Brasil.

Dimensão	Botão municipal convencional	Botão em tornozeleira	Proposta deste trabalho
Discrição em coabitação	Baixa (equipamento dedicado, visualmente identificável)	Média/Baixa (atrelado a tornozeleira do agressor monitorado)	Alta (camuflável em objetos cotidianos)
Cobertura	Área de patrulhamento conveniada	Alcance do monitoramento eletrônico	Onde houver Wi-Fi (extensível a celular/LoRa)
Custo unitário estimado	Centenas a milhares de R\$	Vinculado ao contrato de monitoramento	R\$ 40–60 em materiais
Canais de notificação	Central policial	Central de monitoramento	Painel policial + contatos pessoais via Telegram
Código-fonte	Proprietário	Proprietário	Aberto, adaptável localmente

7.2. Limitações e ressalvas

A análise apresentada possui ressalvas que delimitam o escopo das afirmações deste trabalho:

- **Validação predominantemente em ambiente controlado:** a verificação funcional ocorreu em rede laboratorial; ambientes urbanos reais (residências em uso, casas em diferentes tipologias construtivas), áreas de cobertura instável, locais com forte interferência de RF e quedas prolongadas de energia/Internet não foram caracterizados;
- **Ausência de testes com usuárias e operadores reais:** o protótipo não foi submetido a estudos de usabilidade com mulheres atendidas pela rede de proteção ou com profissionais de DEAMs, CRAMs, polícias militares e guardas civis — etapa que demanda aprovação ética e parceria institucional formal;
- **Indicadores indicativos, não inferenciais:** as métricas reportadas na Seção 5 têm caráter exploratório e não substituem MTBF, taxa de perda sob *stress*, jitter sustentado, disponibilidade longitudinal e análise formal de resiliência de rede;

- **Superioridade afirmada como hipótese:** as dimensões em que a proposta tende a se sobressair (discrição, custo, integração — Tabela 2) decorrem da arquitetura e da literatura, mas só serão confirmadas mediante *benchmarking* direto contra soluções existentes;
- **Dependência de conectividade Wi-Fi,** sem caminho de *fallback* celular (GSM/LTE) ou rádio de longa distância (LoRa) no protótipo atual — limitação parcialmente mitigada pela presença massiva de Wi-Fi em ambientes domésticos;
- **Centralização da geocodificação** no serviço Nominatim/OpenStreetMap, sujeito a limites de uso e à latência de rede;
- **Risco de acionamento involuntário ou induzido** pelo agressor, problema que demanda camadas adicionais de validação contextual;
- **Superfície de ataque na ingestão:** identificação do emissor exclusivamente por UUID, com mitigações de produção (mTLS, HMAC, ACLs MQTT) desenhadas na Seção 4 mas ainda não implementadas no protótipo.

8. Considerações Finais

Este trabalho apresentou o desenvolvimento de um dispositivo discreto de acionamento de emergência para mulheres em situação de violência doméstica, contemplando arquitetura, prototipagem e modelo de distribuição. A motivação central decorre dos números ainda crescentes de feminicídio no Brasil — 1.568 vítimas em 2025 [Fórum Brasileiro de Segurança Pública 2026] — e das limitações operacionais das soluções existentes [Diatchuk e Schuartz 2023], especialmente em cenários de coabitação com o agressor. Ao adotar componentes de baixo custo (ESP-01), software livre (FastAPI, Mosquitto, PostgreSQL, React) e um modelo de distribuição articulado às DEAMs e CRAMs [dos Santos e Cordeiro 2023], a proposta oferece uma alternativa tecnologicamente acessível e operacionalmente integrada às políticas públicas de proteção [dos Santos e Cordeiro 2023, da Conceição da Silva Lima e Rodrigues 2022].

Como contribuições principais, destacam-se: (i) a especificação detalhada de uma arquitetura de hardware e software de baixo custo voltada ao acionamento emergencial discreto; (ii) o protótipo funcional, validado em ambiente controlado; e (iii) um modelo de distribuição que dialoga diretamente com a rede de proteção institucional, evitando a criação de canais paralelos e aproveitando os fluxos já consolidados pela Lei Maria da Penha.

Como trabalhos futuros, identificam-se as seguintes frentes, organizadas para endereçar diretamente as limitações reconhecidas na Seção 7:

- (a) **Testes-piloto em campo** em parceria com municípios e órgãos de segurança pública, com *delineamento experimental formal* — definição de tamanho amostral, métricas objetivas (tempo de resposta, MTBF, taxa de entrega, taxa de perda de pacotes, jitter, disponibilidade, tempo médio de reconexão), análise inferencial e protocolo reproduzível;
- (b) **Caracterização de desempenho em ambientes representativos**, incluindo residências reais em uso, regiões com conectividade intermitente (zonas rurais e periferias), locais com forte interferência de RF (subestações de energia, aglomerados de pessoas, *shoppings*, ambientes com múltiplos *access points* e *roaming*) e cenários de queda prolongada de energia ou Internet;

- (c) **Benchmark comparativo** com as soluções existentes elencadas na Tabela 2 (botão municipal convencional e botão acoplado a tornozelo), contemplando latência, autonomia energética, custo operacional total, taxa de falha e usabilidade;
- (d) **Estudos de usabilidade com usuárias e profissionais** da rede de proteção (DEAMs, CRAMs, polícias militares e guardas civis), condicionados à aprovação em comitê de ética e a parcerias institucionais formais;
- (e) **Endurecimento de segurança** da camada de ingestão, implementando as mitigações desenhadas na Seção 4 — autenticação mútua TLS (mTLS), assinatura HMAC do *payload* e ACLs no broker MQTT — e formalizando o programa de adequação à LGPD com a entidade pública operadora;
- (f) **Fallback de comunicação** via celular (GSM/LTE) ou via radiofrequência longa distância (LoRa), ampliando a cobertura para ambientes externos e regiões sem Wi-Fi;
- (g) **Integração com aplicativos e sistemas oficiais existentes** — como o Botão de Emergência da Lei Maria da Penha, o REDS em Minas Gerais e plataformas estaduais de despacho (CAD) e atendimento (SOS Mulher) —, inserindo o dispositivo na cadeia institucional já consolidada e evitando a criação de canais paralelos;
- (h) **Mecanismos antifraude** para mitigar acionamentos involuntários ou induzidos por terceiros, incluindo camadas de validação contextual; e
- (i) **Estudos longitudinais** sobre o perfil de uso do dispositivo, à luz da proposta metodológica de Diatchuk e Schuartz [Diatchuk e Schuartz 2023], para fundamentar políticas públicas baseadas em evidências.

Em uma evolução natural do projeto, prevê-se a adequação do circuito eletrônico para a fabricação em massa de placas de circuito impresso (PCBs) próprias, projetadas sob medida para a aplicação. A substituição dos módulos de prateleira por uma PCB dedicada permitirá miniaturizar o conjunto para além do que é viável com componentes prontos, com placas mais finas, em formatos variados (circulares, retangulares alongadas, em forma de pílula ou em *flex* contornando superfícies curvas) — viabilizando a integração em uma diversidade ainda maior de *cases* cotidianos, como tubos de batom, embalagens de protetor labial, fivelas de cinto, presilhas e enfeites de cabelo, pingentes e brincos. Essa miniaturização também tende a reduzir o consumo energético do conjunto e ampliar a autonomia da bateria.

No plano da articulação institucional, propõe-se a oferta da solução como projeto-piloto em municípios da região, mediante contato direto com representantes políticos locais (vereadores, prefeituras, secretarias de segurança pública e secretarias da mulher) e com comandantes de companhias da Polícia Militar e da Guarda Civil Municipal. Por se tratar de uma aplicação web, a adoção pelas instituições não exige qualquer instalação adicional ou modificação na infraestrutura de TI existente: a operação ocorre integralmente via navegador, a partir dos próprios computadores e *notebooks* já em uso nas viaturas, salas de operação e centros de comando dos órgãos.

Do lado da hospedagem, a aplicação pode ser implantada tanto em provedores de nuvem pública — como Microsoft Azure, Amazon Web Services ou Google Cloud — quanto em servidores *on-premises* dos próprios órgãos, conforme a política de governança de dados de cada estado ou município. A arquitetura containerizada via *Docker Compose* é portátil entre esses cenários sem alteração de código. Mais relevante, uma única

implantação corretamente dimensionada — em termos de banco de dados, broker MQTT e capacidade do servidor de aplicação — é capaz de atender simultaneamente múltiplas regiões e, no limite, um país inteiro: basta que cada pequeno dispositivo embarcado tenha acesso à Internet para se conectar ao servidor central. Essa característica reforça o potencial da proposta como política pública de alcance nacional, sem depender de implantações regionais redundantes ou de infraestrutura local especializada.

Referências

- da Conceição da Silva Lima, S. e Rodrigues, J. S. (2022). A violência contra a mulher na perspectiva da psicologia: uma revisão bibliográfica. *Revista de Psicologia*, 13(1):139–153.
- Diatchuk, D. C. W. W. e Schuartz, A. S. (2023). Violência contra a mulher: mulheres usuárias do botão do pânico. *Revista Humanidades em Perspectiva*, 5(11):5–19.
- dos Santos, E. G. e Cordeiro, T. L. C. (2023). A violência doméstica e familiar contra a mulher e a (in)eficiência das políticas públicas de prevenção: uma análise na literatura jurídica. *Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)*, 9(5):1834–1853.
- Fórum Brasileiro de Segurança Pública (2026). Retrato dos feminicídios no brasil. Nota técnica, Fórum Brasileiro de Segurança Pública (FBSP), São Paulo.