GOVERNO DO ESTADO DE MINAS GERAIS

POLÍCIA MILITAR DE MINAS GERAIS

Seção de Licitações do Comando de Aviação do Estado

Estudo Técnico Preliminar (ETP) 135562813 - PMMG/COMAVE 4 - LICITAÇÕES

Belo Horizonte, 17 de março de 2026.

1. 1. INFORMAÇÕES GERAIS

1.1. **Número do processo SEI:** 1250.01.0005266/2026-49

1.2. **Equipe de planejamento da contratação:** Conforme ato de designação **135357004**

2. DIAGNÓSTICO DA SITUAÇÃO ATUAL

2.1. **Descrição da necessidade da Administração (PREENCHIMENTO OBRIGATÓRIO)** ***(art. 6º, I e IV, da Resolução Seplag nº 115, de 2021)***

2.1.1. A presente contratação decorre da necessidade de fortalecimento da capacidade institucional de prevenção, detecção, acompanhamento e resposta a ocorrências envolvendo Aeronaves Remotamente Pilotadas (ARP), diante da ampliação objetiva do risco operacional associado ao uso indevido, irregular ou ilícito dessas plataformas em contextos de segurança pública, defesa e proteção de infraestruturas e ativos sensíveis.

2.1.2. A evolução tecnológica do setor, combinada com a ampla disponibilidade de aeronaves remotamente pilotadas no mercado civil, com maior alcance, autonomia, estabilidade de voo, qualidade de transmissão de dados e facilidade de operação, produziu mudança relevante no ambiente de risco enfrentado pela Administração Pública. Em consequência, atividades ilícitas, antes dependentes de maior complexidade logística, passaram a poder ser executadas com menor custo, maior discrição, elevada mobilidade e dificuldade acrescida de pronta intervenção pelos meios convencionais de vigilância e proteção.

2.1.3. No contexto nacional, dados públicos da Agência Nacional de Aviação Civil (ANAC) indicavam, em 2025, cerca de 125 mil drones cadastrados no Sistema de Aeronaves Não Tripuladas (SISANT). Tal crescimento quantitativo, embora compatível com usos lícitos e economicamente relevantes da tecnologia, amplia, por consequência, a exposição da Administração a eventos de uso indevido ou malicioso, sobretudo em áreas urbanas, instalações críticas, eventos públicos e operações sensíveis.

2.1.4. Antes mesmo da análise dos cenários setoriais específicos, cumpre registrar que já há, no Brasil, ocorrências documentadas de emprego de drones por grupos criminosos para monitorar, em tempo real, deslocamentos e ações de forças de segurança em contexto operacional. Em janeiro de 2025, reportagem da CNN Brasil registrou caso em que traficantes monitoravam, por drone, a atuação do 9º Batalhão, em operação realizada pela Polícia Militar no Rio de Janeiro. Em setembro de 2024, a Polícia Federal, na Operação Buzz Bomb, informou que drones de organização criminosa no Rio de Janeiro foram utilizados tanto em ataques com artefatos explosivos quanto para monitorar ações policiais no Complexo da Penha e em outras áreas dominadas pelo grupo. No mesmo sentido, investigações noticiadas em 2025 apontaram o emprego de drones para monitorar tropas policiais e orientar ataques contra rivais e agentes públicos, enquanto documento oficial do Estado do Rio de Janeiro também registra episódios em que facções passaram a utilizar drones para monitorar operações policiais, transportar materiais ilícitos e planejar ataques contra agentes de segurança pública. Esse quadro demonstra que, no cenário brasileiro, o drone já se consolidou em determinados ambientes criminais como ferramenta tática de vigilância, antecipação, coordenação e reação contra ações policiais ostensivas, o que repercute diretamente na realidade operacional das Polícias Militares e reforça a pertinência de solução móvel apta ao emprego dinâmico em campo.

2.1.5. A necessidade administrativa mostra-se ainda mais evidente diante da recorrência de ocorrências envolvendo drones em cenários de alta sensibilidade operacional, entre os quais se destacam:

2.1.6. **Eventos de massa e proteção de autoridades:** grandes eventos, solenidades, operações especiais e atividades envolvendo dignitários, autoridades ou públicos numerosos apresentam elevada sensibilidade a incursões aéreas não autorizadas. Nesses contextos, drones podem ser empregados para captação indevida de imagens, perturbação da ordem, transporte de cargas perigosas, reconhecimento prévio ou ação hostil direta. Caso internacional recente demonstra a relevância operacional de arquiteturas distribuídas de sensoriamento integradas a estruturas centralizadas de coordenação: em Barcelona, a polícia catalã estruturou zona de proteção aérea de aproximadamente 50 km² e, durante a Fórmula 1 de 2022, respondeu a 260 alertas de drones ao longo de três dias, distinguindo aeronaves autorizadas e não autorizadas em ambiente de grande concentração de público.

2.1.7. **Faixa de fronteira e criminalidade organizada:** há risco concreto de utilização de drones por organizações criminosas para transporte de entorpecentes e outros ilícitos, vigilância de rotas, monitoramento de deslocamentos de forças de segurança e apoio a ações logísticas clandestinas. Tal cenário incrementa a complexidade das ações de fiscalização, repressão e patrulhamento, exigindo ampliação da consciência situacional e da capacidade de antecipação por parte do poder público. Estudo publicado em portal oficial do Governo Federal já apontava o aperfeiçoamento do uso de VANT por grupos criminosos em práticas como tráfico de drogas e armas, monitoramento de áreas de interesse e enfrentamento às forças de segurança.

2.1.8. **Ameaças emergentes, inclusive drones FPV e plataformas adaptadas ou artesanalmente configuradas:** conflitos recentes e experiências operacionais contemporâneas evidenciaram a crescente utilização de drones FPV e de plataformas improvisadas ou modificadas como vetores de observação, perturbação e ataque. Em fevereiro de 2026, a Reuters reportou que pequenos drones FPV passaram a dominar parcelas relevantes do campo de batalha na Ucrânia. Em paralelo, experiências operacionais no mesmo teatro indicaram a adoção de redes distribuídas de sensores portáteis, inclusive com conectividade satelital, instaladas ao longo da linha de frente para operação contínua. Tais referências demonstram que o risco não se restringe a modelos comerciais padronizados, alcançando também configurações não convencionais, de rápida adaptação e elevada variabilidade técnica.

2.1.9. Desse modo, a necessidade pública subjacente não se confunde com a mera aquisição de bens ou ferramentas isoladas, mas consiste na estruturação de **capacidade operacional móvel,** compatível com o atual cenário de risco e apta ao emprego em operações da Polícia Militar, especialmente em contextos dinâmicos, descentralizados e de pronta resposta, com o objetivo de elevar a consciência situacional, apoiar a identificação tempestiva de incursões aéreas não autorizadas, subsidiar a resposta institucional e reduzir a exposição de pessoas, serviços, instalações e ativos estratégicos da Administração.

2.1.10. Sob a perspectiva do interesse público, a contratação justifica-se pela necessidade de prevenir danos à segurança institucional, mitigar vulnerabilidades operacionais, ampliar a capacidade de proteção de ambientes sensíveis e assegurar condições mínimas para atuação estatal eficaz diante de ameaça concreta, atual e progressivamente mais sofisticada.

2.1.11. **Necessidade operacional:** Identifica-se necessidade operacional imediata e inadiável de dotar a PMMG/COMAVE, especialmente para emprego em operações da Polícia Militar, de capacidade integrada de Detecção, Rastreamento, Identificação e Mitigação (DTI-M) em configuração móvel e portátil, apta a apoiar ações em campo, missões de pronta resposta, operações especiais, policiamento em áreas urbanas sensíveis, proteção de autoridades, grandes eventos, cumprimento de mandados, incursões em áreas conflagradas e demais cenários em que a ameaça representada por aeronaves remotamente pilotadas exija resposta tempestiva, coordenada e tecnicamente qualificada.

2.1.12. A necessidade não se limita à disponibilidade de equipamento isolado, mas abrange a estruturação de capacidade operacional efetiva, interoperável e escalável, apta a funcionar em contexto real de segurança pública, com mobilidade tática, comando centralizado, emprego distribuído e suporte à decisão em tempo oportuno. Considerando a dinâmica das operações policiais militares, a solução pretendida deverá permitir rápida projeção em campo, operação em ambientes complexos de radiofrequência, identificação de múltiplos perfis de ameaça, apoio à localização do operador remoto, registro probatório dos eventos e integração entre sensoriamento, comando e mitigação.

2.1.13. Nesse contexto, a capacidade operacional requerida deverá atender, cumulativa e simultaneamente, às seguintes necessidades:

2.1.14. **Desdobramento rápido e emprego expedito:** a solução deverá permitir montagem, configuração inicial e entrada em operação em prazo compatível com a dinâmica das ações policiais, preferencialmente em **até 15 (quinze) minutos,** sem dependência de infraestrutura civil prévia, obras, cabeamento estruturado permanente ou preparação complexa do local. Tal requisito decorre da necessidade de emprego em operações móveis, temporárias, contingenciais ou de oportunidade, nas quais a velocidade de instalação é fator crítico para a utilidade operacional do sistema.

2.1.15. **Operação eficaz em ambiente urbano e eletromagneticamente complexo:** a solução deverá operar com efetividade em ambientes urbanos densos e com elevada saturação de sinais de radiofrequência, inclusive na presença de redes Wi-Fi, Bluetooth, enlaces de dados, sistemas celulares e outras fontes de emissão eletromagnética. Deverá, ainda, empregar mecanismos técnicos adequados para filtragem, seleção, priorização e tratamento de sinais, de modo a reduzir falsos positivos, aumentar a confiabilidade dos eventos e minimizar interferências colaterais decorrentes da operação em áreas povoadas e sensíveis.

2.1.16. **Cobertura de ameaças atuais e emergentes:** a capacidade pretendida deverá abranger não apenas drones comerciais amplamente difundidos, mas também plataformas FPV, configurações DIY, aeronaves adaptadas, sistemas com perfis de emissão não convencionais e ameaças emergentes, inclusive aquelas que reflitam a rápida evolução do cenário tecnológico e criminal. O requisito decorre da constatação de que o risco operacional não se restringe a modelos padronizados de mercado, alcançando também plataformas improvisadas, modificadas ou empregadas com finalidade hostil em contextos dinâmicos.

2.1.17. **Integração ponta a ponta da cadeia DTI-M:** a necessidade operacional compreende solução apta a suportar fluxo integrado e contínuo entre sensoriamento, comando e ação, permitindo encadeamento funcional entre sensores, plataforma de comando e controle e efetores de mitigação. Busca-se, com isso, reduzir o tempo entre detecção e resposta, ampliar a consistência da tomada de decisão e viabilizar a cadeia de atuação e mitigação, com suporte a processos automatizados e, quando aplicável, a mecanismos de smart jamming com protocolo específico orientados pelas informações qualificadas obtidas pelo sistema.

2.1.18. **Localização do piloto e apoio à interceptação policial:** a solução deverá prover elementos que permitam determinar, com o maior grau possível de precisão operacional, a posição do operador remoto ou da fonte de controle da aeronave, de modo a subsidiar a pronta atuação das equipes policiais em solo. A necessidade não se limita, portanto, à identificação do drone em voo, mas alcança também a produção de dados úteis à abordagem, interceptação, contenção e responsabilização do agente envolvido na conduta ilícita.

2.1.19. **Capacidade de registro e preservação de evidências:** a solução deverá registrar automaticamente os eventos relevantes, alarmes, trilhas de operação, dados de detecção, parâmetros associados à ocorrência e demais elementos pertinentes, em formato apto a apoiar análise posterior, reconstrução dos fatos, inteligência policial e materialidade probatória. Trata-se de requisito essencial para permitir aproveitamento administrativo, operacional e, eventualmente, judicial das informações produzidas, reforçando a cadeia de custódia informacional e a rastreabilidade das ocorrências.

2.1.20. **Operação remota, centralizada e escalável:** a necessidade operacional do órgão demandante pressupõe arquitetura que permita operar sensores de forma distribuída e **remota**, sem necessidade de operador presencial dedicado em cada ponto de detecção, com monitoramento centralizado no Comando de Aviação do Estado (ComAvE). O cenário operacional pretendido compreende implantação gradual de sensores em pontos estratégicos do Estado, inicialmente em configuração móvel/portátil e, à medida que se consolide a maturidade operacional, também em arranjos semifixos ou fixos, todos geridos remotamente por equipes especializadas do ComAvE. Nesse modelo, as equipes táticas de campo, dotadas dos efetores de mitigação, serão acionadas sob demanda a partir das informações produzidas pela plataforma em tempo real, inclusive azimute, direção de aproximação e elementos de geolocalização, deslocando-se ao ponto de ameaça conforme a necessidade operacional. Tal modelo permite ampliar progressivamente a malha de sensoriamento em âmbito estadual sem exigir acréscimo proporcional de efetivo especializado em cada localidade monitorada, favorecendo racionalidade administrativa, padronização operacional, economia de meios e ganho de escala.

2.1.21. Além dos aspectos acima, a necessidade operacional deve ser compreendida à luz da realidade própria das operações policiais militares, marcadas por mobilidade, imprevisibilidade, dispersão territorial, limitação de tempo para preparação, necessidade de coordenação entre diferentes frações e exigência de resposta segura em cenários de risco elevado. Por essa razão, a capacidade a ser estruturada deverá combinar prontidão, mobilidade, confiabilidade técnica, centralização do comando e flexibilidade de emprego, permitindo tanto o uso pontual em missões específicas quanto sua evolução para uma rede ampliada de monitoramento aéreo tático em

apoio à segurança pública estadual.

2.1.22. Desse modo, a necessidade operacional do órgão demandante consiste em dispor de solução móvel/portátil de capacidade DTI-M que não apenas detecte ameaças aéreas não autorizadas, mas que efetivamente se integre ao ciclo decisório e à resposta policial, viabilizando monitoramento remoto centralizado, emprego distribuído em campo, apoio à mitigação, localização de operadores, produção de provas e expansão escalável da cobertura operacional no território estadual.

2.2. **Alinhamento entre a demanda (potencial contratação) e o planejamento da Administração *(art. 6º, II, da Resolução Seplag nº 115, de 2021)***

2.2.1. A presente demanda não foi planejada por esta unidade solicitante durante a elaboração e as revisões do plano de contratações anual para o exercício corrente em razão da natureza extraordinária da disponibilidade orçamentária para o setor. A Polícia Militar de Minas Gerais recebe recorrentemente aportes de recursos de variadas fontes externas, tais como emendas parlamentares, convênios estaduais e federais, além de doações de entes públicos e privados, o que impossibilita a previsão exata do montante e da data de disponibilização financeira no momento da elaboração do Plano de Contratações Anual (PCA).

2.2.2. Ocorre que, conforme disposto no Memorando nº 600.017.2/2026 - EMPM, com a publicação do Decreto NE nº 188, de 26 de fevereiro de 2026, do Governo do Estado de Minas Gerais, no qual consta a suplementação de crédito à PMMG vinculada ao Programa de Pleno Pagamento de Dívidas dos Estados – PROPAG, foi disponibilizado o recurso de capital na ordem de R$ 11.287.267,64 (onze milhões, duzentos e oitenta e sete mil, duzentos e sessenta e sete reais e sessenta e quatro centavos) destinado à aquisição dos itens de materiais permanentes para o COMAVE. Nesse sentido, o comando geral da instituição determinou a aquisição de drones e sistema antidrone para uso na atividade policial conforme justificado no item 2.1 do presente documento.

2.3. **Descrição dos requisitos da potencial contratação necessários e suficientes à escolha da solução *(art. 6º, III, da Resolução Seplag nº 115, de 2021)***

2.3.1. A opção por solução em configuração móvel/portátil decorre das características concretas do ambiente operacional da Polícia Militar e da natureza dinâmica, difusa e mutável das ameaças associadas ao uso indevido de Aeronaves Remotamente Pilotadas (ARP). **Em tal contexto, a necessidade institucional não se concentra, ao menos em sua fase inicial, na proteção exclusiva de um único ponto fixo ou de uma instalação permanentemente delimitada, mas na capacidade de projetar meios técnicos de detecção, acompanhamento, identificação e resposta para diferentes locais do território estadual, conforme a evolução do risco, a criticidade da missão e a inteligência operacional disponível.**

2.3.2. A realidade das operações policiais militares é marcada por mobilidade, imprevisibilidade, necessidade de pronta resposta e frequente alteração do teatro de operações. Missões de apoio aéreo, cumprimento de mandados, operações em áreas conflagradas, grandes eventos, escoltas, proteção de autoridades, ações em estabelecimentos sensíveis e respostas emergenciais demandam capacidade que possa ser rapidamente deslocada, instalada, operada e reposicionada sem dependência de infraestrutura prévia complexa. **Nessa perspectiva, a solução móvel/portátil mostra-se mais aderente ao interesse público do que modelos exclusivamente fixos na etapa atual de estruturação da capacidade.**

2.3.3. A justificativa técnica e operacional para a adoção dessa configuração assenta-se, cumulativamente, nos seguintes fundamentos:

1. **Adequação ao perfil das operações da Polícia Militar:** as missões policiais não se desenvolvem apenas em pontos permanentes e previsíveis, mas frequentemente em cenários temporários, mutáveis e distribuídos geograficamente. A solução móvel/portátil permite acompanhar essa dinâmica, sendo empregada conforme a demanda operacional, inclusive em áreas nas quais não seria razoável ou economicamente eficiente manter infraestrutura fixa permanente.
2. **Pronta resposta e flexibilidade de emprego:** a capacidade de montagem rápida e operação sem preparação prévia extensa permite o uso do sistema em missões emergenciais, planejadas ou de oportunidade. Trata-se de atributo essencial para situações em que a utilidade operacional depende da rapidez de desdobramento, da possibilidade de relocalização e da adaptação a cenários supervenientes.
3. **Compatibilidade com o caráter não estático da ameaça:** o uso ilícito de drones por organizações criminosas e outros agentes hostis não se limita a instalações permanentes, podendo ocorrer em deslocamento, em operações pontuais, em áreas urbanas sensíveis, em rotas de interesse policial, em perímetros temporariamente protegidos e em missões especiais. A solução móvel/portátil é mais compatível com esse padrão de ameaça do que uma arquitetura inicialmente restrita a posições fixas.
4. **Possibilidade de cobertura de múltiplos cenários com o mesmo conjunto de meios:** ao permitir o deslocamento da capacidade entre diferentes regiões, operações e tipos de missão, a configuração móvel/portátil amplia o aproveitamento do investimento público, evitando a imobilização de recursos técnicos em locais de uso exclusivamente permanente e permitindo atendimento de demandas variadas com maior racionalidade administrativa.
5. **Redução de dependência de obras e infraestrutura civil:** soluções fixas, em regra, exigem intervenções de engenharia, adequações físicas, pontos dedicados de energia, conectividade permanente, autorizações locais e prazos maiores de implantação. A configuração móvel/portátil reduz essas dependências, acelera a disponibilização da capacidade operacional e mitiga entraves administrativos e logísticos típicos de implantações estruturais.
6. **Menor prazo de entrada em operação da capacidade institucional:** a Administração possui interesse em estruturar capacidade utilizável no curto prazo, especialmente diante da atualidade da ameaça. A solução móvel/portátil permite antecipar o emprego operacional do sistema, reduzindo o intervalo entre contratação, capacitação, testes e efetiva utilização em campo.
7. **Viabilidade de implantação gradual e amadurecimento doutrinário:** a configuração móvel/portátil permite que a instituição desenvolva progressivamente sua doutrina de emprego, refine procedimentos operacionais, avalie áreas prioritárias, consolide fluxos entre comando e campo e adquira maturidade técnica antes da eventual expansão para arranjos semifixos ou fixos. Trata-se, portanto, de modelo compatível com implementação escalonada, aprendizado institucional e gestão prudente do investimento público.

2.3.4. Ressalta-se, por fim, que a escolha pela configuração móvel/portátil não exclui a possibilidade de, em etapas futuras, a Administração adotar arranjos semifixos ou fixos em pontos de criticidade permanente. Ao contrário, a solução ora justificada deve ser compreendida como etapa inicial e estruturante de um modelo mais amplo de capacidade operacional, no qual a mobilidade, a centralização do comando, a escalabilidade e a flexibilidade de emprego constituem requisitos prioritários para atendimento do interesse público.

3. PROSPECÇÃO DE SOLUÇÕES

3.1. **Levantamento de mercado (PREENCHIMENTO OBRIGATÓRIO)** ***(art. 6º, V, da Resolução Seplag nº 115, de 2021)***

3.1.1. **NECESSIDADE DE AQUISIÇÃO INTERNACIONAL:** A presente contratação demanda análise específica quanto à necessidade de aquisição internacional, não por preferência subjetiva por fornecedor estrangeiro, mas em razão da natureza do objeto definido no planejamento. A Lei nº 14.133/2021 distingue a licitação internacional — processada em território nacional com admissão de licitantes estrangeiros — das contratações realizadas no exterior, e o TCU ressalta essa diferenciação conceitual ao examinar a matéria. No caso concreto, a necessidade ora tratada refere-se, substancialmente, à aquisição de solução de origem tecnológica estrangeira, sem afastamento da incidência da legislação brasileira de contratações públicas, do controle jurídico nacional e das exigências regulatórias aplicáveis no Brasil.

3.1.2. **RAZÕES TÉCNICAS PARA IMPOSIÇÃO DA AQUISIÇÃO INTERNACIONAL:** A necessidade de aquisição internacional decorre, em primeiro lugar, do fato de que o objeto não se resume a bens físicos isolados, passíveis de nacionalização simplificada ou substituição por equivalentes genéricos. Trata-se de solução C-UAS móvel/portátil integrada, composta por sensor, efetor de mitigação, plataforma de comando e controle em nuvem, biblioteca proprietária de assinaturas de radiofrequência, firmware, protocolos internos de comunicação, rotinas de classificação, lógica de direcionamento de engajamento, trilhas de auditoria, mecanismos de atualização centralizada e suporte evolutivo coordenado.

3.1.3. Os elementos centrais dessa solução — especialmente a biblioteca proprietária de assinaturas RF, a lógica integrada entre sensoriamento, classificação, comando e mitigação, a instância em nuvem da plataforma C2 e o ciclo contínuo de atualização tecnológica — são, por sua natureza, ativos imateriais e tecnológicos controlados pelo ecossistema original da solução. Não se trata, portanto, de objeto que possa ser reproduzido licitamente no mercado nacional por mera integração de componentes de terceiros, montagem local ou substituição parcial de subsistemas sem alteração da identidade funcional do objeto definido no planejamento.

3.1.4. A aquisição internacional mostra-se necessária porque a efetividade da solução depende do acesso direto e contínuo ao ecossistema tecnológico original, inclusive no que se refere a atualizações de software e firmware, evolução da biblioteca de assinaturas, manutenção da compatibilidade entre os componentes, correções de segurança cibernética, suporte especializado e preservação do desempenho nominal do sistema. A tentativa de converter esse fornecimento em contratação puramente nacional, por meio de composição artificial entre múltiplos fornecedores ou por nacionalização incompleta do objeto, acarretaria alteração substancial da solução técnica requerida.

3.1.5. **INEXISTÊNCIA DE ALTERNATIVA NACIONAL EQUIVALENTE PARA O OBJETO DEFINIDO** : A necessidade de aquisição internacional não significa afirmar que inexistam, em abstrato, empresas nacionais capazes de fornecer componentes, acessórios, integração ou apoio logístico. O ponto juridicamente e tecnicamente relevante é outro: o objeto definido neste ETP exige solução unitária, integrada, nativa e funcionalmente indivisível, e não mera reunião de itens similares ou parcialmente compatíveis.

3.1.6. Mesmo que existam no mercado nacional distribuidores, integradores, representantes comerciais ou fornecedores de subsistemas correlatos, isso não elimina a natureza internacional da aquisição quando o núcleo tecnológico da solução — desenho arquitetural, biblioteca proprietária, software crítico, firmware, protocolos internos, direitos de propriedade intelectual, ambiente em nuvem e capacidade evolutiva — permanece sediado, controlado e disponibilizado a partir do exterior. Em tais circunstâncias, o fornecimento local, quando existente, atua apenas como braço comercial, logístico, técnico ou representativo do ecossistema original, sem desnaturar a origem internacional do objeto.

3.1.7. Também não se mostra adequada a exigência de produção nacional como condição para a contratação. A solução pretendida não se esgota na materialidade dos equipamentos; ela depende de acervo tecnológico, base de conhecimento proprietária, validação operacional acumulada, cadeia evolutiva de software e integração nativa entre subsistemas. A substituição dessa arquitetura por arranjos localmente compostos implicaria modificação do objeto, perda de desempenho, aumento de risco operacional e ruptura da coerência técnica já demonstrada ao longo deste ETP.

3.1.8. **COMPATIBILIDADE DA AQUISIÇÃO INTERNACIONAL COM O INTERESSE PÚBLICO** : A aquisição internacional, no presente caso, é compatível com o interesse público porque preserva a identidade do objeto, reduz o risco de degradação funcional da solução e assegura aderência aos requisitos críticos definidos pela Administração. Em vez de representar opção excepcional por simples origem estrangeira, ela constitui medida necessária para garantir que a Administração receba exatamente a capacidade operacional de que necessita, e não aproximação imperfeita dessa capacidade.

3.1.9. Sob a ótica econômica e contratual, a aquisição internacional também pode revelar-se mais vantajosa quando comparada a arranjos internos artificiais. Isso porque a contratação vinculada ao ecossistema original tende a preservar a coerência entre preço, garantia, atualização, suporte, treinamento, licenciamento, escalabilidade e continuidade operacional. Em objetos tecnologicamente complexos, a multiplicação de intermediários nacionais, integradores paralelos ou camadas contratuais adicionais tende a elevar custos indiretos, ampliar zonas de conflito de responsabilidade e dificultar a sustentação da solução ao longo do tempo.

3.1.10. Diante do exposto, conclui-se que a aquisição internacional é necessária para o atendimento da necessidade administrativa descrita neste ETP. Tal necessidade decorre da origem estrangeira do ecossistema tecnológico requerido, da indisponibilidade de alternativa nacional equivalente capaz de reproduzir, de forma lícita e funcionalmente íntegra, a solução definida no planejamento, e da exigência de preservação da integração nativa entre sensores, plataforma C2, biblioteca proprietária, lógica de classificação e efetor de mitigação.

3.1.11. A contratação internacional, nesse contexto, não representa preferência por procedência estrangeira, mas consequência técnica da própria definição do objeto. A tentativa de substituí-la por arranjo artificialmente nacional implicaria descaracterização da solução, aumento de risco operacional, perda de desempenho, ruptura da unidade tecnológica e comprometimento da finalidade pública perseguida. Por isso, a origem internacional do fornecimento deve ser tratada como atributo necessário do objeto, sem prejuízo da observância integral do regime jurídico brasileiro, das exigências regulatórias nacionais e, quando cabível, da atuação de representante ou estrutura de suporte local formalmente autorizados pelo ecossistema original da solução.

3.1.12. Com base no levantamento de mercado, na análise comparativa das alternativas, nas respostas ao instrumento padronizado de consulta, na documentação técnica apresentada e nas diligências realizadas, conclui-se que a solução **Dedrone by Axon** comprovou, de forma integral, cumulativa e simultânea, o atendimento aos requisitos críticos e técnicos definidos neste Estudo Técnico Preliminar. A documentação analisada demonstra, entre outros pontos, integração entre sensores RF passivos, plataforma DedroneTracker.AI e efetor de mitigação inteligente; orientação de engajamento em tempo real; mitigação protocolo-específica com apoio de inteligência artificial;

operação com sensores cloud-ready; e capacidade de localizar drones e respectivos operadores em mapa georreferenciado.

> *O RF-560, integrante do ecossistema ofertado, é descrito como sensor de longo alcance, passivo, preparado para operação em nuvem, apto à detecção e classificação de sinais de radiofrequência nas faixas de 2,4 GHz, 5,2 GHz e 5,8 GHz, com recepção de Remote ID, alcance típico de 5 km com antenas omnidirecionais e 8 km com antenas direcionais, operação via navegador por meio do DedroneTracker.AI e atualizações de firmware e da biblioteca DedroneDNA providas pelo fabricante.*
>
> *O RF-360, por sua vez, é descrito como sensor passivo, omnidirecional, com capacidade de direction finding por radiofrequência e Wi-Fi, detecção e classificação de sinais e, em combinação com duas ou mais unidades, determinação da posição do drone e do controle remoto, com envio de dados e alertas ao DedroneTracker.AI por conexão móvel ou LAN. Seu alcance nominal é de 2 km para a maioria dos drones, podendo atingir até 5 km em condições ideais, com conectividade integrada e operação por interface baseada em navegador.*
>
> *O DedroneDefender 2, por sua vez, é apresentado como jammer de protocolo alimentado por IA, integrado ao DedroneTracker.AI, com guidance display em tempo real, cone efetivo de 20°, jamming narrowband orientado ao protocolo identificado, capacidade anti-swarm, cobertura de bandas ISM e GNSS, operação com bateria AN/PRC-148 e emprego previsto tanto em defesa de linha de frente quanto em segurança urbana.*

3.1.13. Também ficou evidenciado que a plataforma DedroneTracker.AI opera por interface browser-based, com visualização em mapa, alertas em tempo real, notificações por e-mail, SMS, SNMP, TCP/IP e JSON, armazenamento de dados para playback e reporting, além de funções de exportação, relatórios programados e trilhas de auditoria.

3.1.14. À vista desse conjunto, adota-se, nesta seção conclusiva, a premissa de que os requisitos definidos neste ETP foram comprovadamente atendidos pela solução **Dedrone by Axon**, com documentação idônea, coerente e tecnicamente suficiente.

3.1.15. Diante da possibilidade real de que haja no mercado mais de uma empresa apta a fornecer a tecnologia referenciada, faz-se necessário lançar pregão eletrônico visando a aquisição pretendida.

3.1.16. Destaca-se ainda que a **Dedrone by Axon** trata-se de uma solução apenas referencial, sendo que nada impede que outras tecnologias sejam contratadas desde atendam aos requisitos técnicos exigidos e justificados.

3.1.17. Assim, a pergunta juridicamente relevante não é se existem, em abstrato, sensores RF, softwares de monitoramento, radares, jammers ou integradores no mercado. A pergunta relevante é se existe pluralidade real de agentes econômicos aptos a fornecer, hoje, de forma nativa, **documentada, simultânea e comprovada**, a totalidade do objeto definido pela Administração. À luz da premissa adotada nesta instrução, a **resposta é positiva,** razão pela qual resta configurada a viabilidade de competição para o objeto em sua integralidade.

3.2. **Estimativa dos custos das soluções (PREENCHIMENTO OBRIGATÓRIO)** ***(art. 6º, VI, da Resolução Seplag nº 115, de 2021)***

3.3. Primeiramente, quanto ao quantitativo para a presente contratação, foi estabelecido o quantativo do item 4.5.13. para suprir a necessidade de estruturação de uma capacidade operacional mínima e autossuficiente para a Polícia Militar de Minas Gerais (PMMG). Dado que o Estado de Minas Gerais possui vasta extensão territorial e demandas simultâneas em grandes eventos, proteção eventual em presídios e operações em áreas conflagradas (tais como: ataques do "Novo Cangaço") , a aquisição de 03 unidades do "Lote 01" (kit completo) e 03 unidades do "Lote 02" permite o desdobramento tático imediato de pronta resposta em pontos geograficamente distintos, garantindo que a detecção seja imediatamente sucedida pela capacidade de neutralização inteligente, sem as quais a missão de segurança pública restaria ineficaz frente às ameaças aéreas atuais. Logo, as unidades solicitadas não representam mera reserva de estoque, mas sim o requisito técnico mínimo para viabilizar a radiogoniometria e a triangulação necessária à interceptação policial e à persecução penal dos infratores, permitindo, inicialmente, que a PMMG gerencie uma malha de monitoramento remoto centralizado com alta acurácia operacional.

3.4. Sob a ótica da governança e da racionalidade administrativa, a aquisição destes nove itens (divididos em dois lotes) configura uma "etapa estruturante" de amadurecimento doutrinário para a corporação. Considerando a complexidade tecnológica da solução, o quantitativo proposto é comedido e proporcional ao estágio inicial de implementação da capacidade contra-UAS (C-UAS) na PMMG. Esse número permite o treinamento do efetivo especializado do Esquadrão HARPIA e a avaliação de desempenho em cenários reais antes de uma futura expansão para o restante do território mineiro, evitando-se tanto a obsolescência tecnológica precoce quanto o desperdício de recursos públicos, em estrita observância ao planejamento estratégico da Administração.

3.5. Por fim, a justificativa do quantitativo também se sustenta na necessidade de garantir a continuidade do serviço público de segurança aérea diante da dinâmica das operações policiais militares, que são marcadas pela imprevisibilidade e mobilidade. A disponibilidade de três kits completos do lote 01 e três sensores do lote 02 assegura que, em caso de manutenção técnica ou atualização de firmware em uma das unidades, a corporação não perca sua capacidade de cobertura em missões críticas, como a proteção de autoridades e o monitoramento de infraestruturas sensíveis. Portanto, o montante pretendido guarda total correlação com o diagnóstico de risco apresentado no presente Estudo Técnico Preliminar, mostrando-se necessário para que a PMMG atue no cenário atual face à vulnerabilidade frente ao uso ilícito de drones por organizações criminosas e garanta a integridade das operações terrestres e aéreas sob sua responsabilidade.

3.6. Conforme orçamento apresentado pela empresa AXON ENTERPRISE, INC. 136869558 para a aquisição pretendida estima-se os seguintes custos:

ITEM	PRODUTO	PREÇO UNIT. DE LISTA (USD)	DESCONTO (USD)	PREÇO UNIT. FINAL (USD)
1	Axon Dedrone — Defender Software (licença 60 meses)	54.246,00	4.246,00	50.000,00
2	DedroneDefender 2 — Smart Jammer Portátil (hardware)	75.000,00	30.000,00	45.000,00
3	Axon Dedrone RF-560 — Sensor RF de Longo Alcance (hardware)	30.000,00	—	30.000,00
4	Axon Dedrone — DedroneTracker.AI RF Software Hosted (licença 60 meses, por sensor)	40.684,80	684,80	40.000,00
5	Axon Dedrone — DedroneTracker.AI Software C2 Online (licença 60 meses, por instância)	81.369,60	41.369,60	40.000,00
6	Axon Dedrone RF-360 — Sensor RF Compacto com DF (hardware)	16.500,00	1.500,00	15.000,00
7	Axon Dedrone Battery 600Wh	1.700,00	—	1.700,00
8	Hard Case ruggedizado para transporte de sensores	5.000,00	2.000,00	3.000,00
9	Axon Dedrone Portable (Tactical) Tripod — Base	8.500,00	—	8.500,00
10	Treinamento (20 horas-aula)	10.000,00	—	10.000,00

3.7. **Análise comparativa das alternativas e escolha da solução (PREENCHIMENTO OBRIGATÓRIO)** ***(consequência dos incisos V e VI do art. 6º da Resolução Seplag nº 115, de 2021)***

3.7.1. **CARACTERÍSTICAS TÉCNICAS INDISPENSÁVEIS AO OBJETO**: Uma solução C-UAS adequada ao contexto da PMMG deve necessariamente reunir as seguintes capacidades, cada uma vinculada a uma necessidade operacional concreta e a um risco demonstrável em caso de ausência:

Kill chain DTI-M integrada e automatizada: A cadeia de resposta deve ser executada como fluxo automatizado desde a detecção do sinal RF até a emissão do sinal de disrupção, sem depender de decisão manual do operador para seleção de protocolo ou frequência. A ausência dessa integração resulta em engajamentos lentos, imprecisos, sem rastreabilidade e vulneráveis a erro humano em cenários de múltiplas ameaças simultâneas.

Jamming protocolo-específico (narrowband/smart): Em ambiente de segurança pública urbana, onde comunicações de rádio policial, sistemas GPS de viaturas, redes Wi-Fi de câmeras de vigilância e sistemas de emergência coexistem com as frequências de drones hostis, o único método de neutralização aceitável é aquele que atua exclusivamente no protocolo de comunicação da aeronave-alvo. O jamming broadband — que bloqueia todas as bandas simultaneamente — é incompatível com operações urbanas e expõe o órgão contratante a responsabilidade regulatória nos termos da Resolução ANATEL nº 760/2023.

Geolocalização do operador do drone: A resposta C-UAS não pode se limitar à neutralização da aeronave. Para que a ação policial seja completa, a solução deve fornecer coordenadas acionáveis do piloto em tempo real, com precisão suficiente para direcionamento de equipe terrestre ao local. Sistemas que indicam apenas direção aproximada (bearing) são insuficientes para esse fim.

Operação autônoma sem operador local: O modelo operacional sustentável para uma corporação policial estadual requer que os sensores de detecção operem de forma autônoma e contínua, transmitindo dados para um centro de comando centralizado, sem que cada ponto de detecção demande um policial dedicado em campo permanentemente. Equipamentos handheld que só funcionam com operador presente são incompatíveis com cobertura territorial ampla e permanente.

Biblioteca abrangente com cobertura de ameaças não convencionais: O portfólio de drones utilizados para fins criminosos inclui plataformas FPV artesanais, equipamentos DIY com protocolos modificados e sistemas importados sem identificação comercial — precisamente os modelos que atores criminosos utilizam por serem mais difíceis de detectar. Uma biblioteca que cobre apenas 'modelos convencionais' está por definição defasada ante as ameaças mais relevantes.

Registro forense auditável com cadeia de custódia digital: Cada evento de detecção e neutralização deve gerar, automaticamente, documentação técnica estruturada e rastreável: modelo identificado, protocolo, trajetória, geolocalização do operador, parâmetros do engajamento. Sem esse registro, a ação policial não pode ser documentada para instrução de inquéritos, e o drone neutralizado não contribui para a cadeia probatória contra o infrator.

3.7.2. **ANÁLISE TÉCNICA: DroneShield Ltda. (RFPatrol + DroneGun Tactical):**

3.7.3. O kit DroneShield analisado compõe-se do sensor de detecção portátil RFPatrol e do neutralizador DroneGun Tactical, produzidos pela DroneShield Ltd. (Austrália/EUA).

3.7.4. Falha Estrutural: Ausência de Kill-Chain Integrada. O RFPatrol e o DroneGun Tactical são equipamentos completamente desvinculados. Não existe qualquer protocolo de comunicação entre eles, não há plataforma de C2 que integre os dois componentes e não há fluxo automatizado de targeting. O operador detecta uma ameaça no RFPatrol e decide individualmente, com base apenas na leitura visual do equipamento, quando e como engajar com o DroneGun. Essa ausência de integração sistêmica é uma falha estrutural que compromete todos os demais critérios operacionais, pois não há base técnica para automação, registro forense, coordenação de múltiplas equipes ou gerenciamento centralizado.

3.7.5. Implicação operacional: Em cenário de ameaça múltipla simultânea — enxame de drones —, o operador do kit DroneShield precisa, sem qualquer suporte de IA, detectar, priorizar, apontar e engajar cada ameaça individualmente. A carga cognitiva sobre o operador singular em campo é incompatível com a velocidade e complexidade desse cenário. O RFPatrol exige um policial em campo para cada ponto de detecção, 24 horas por dia. Para cobrir 10 pontos estratégicos do estado — presídios, infraestruturas críticas, locais de eventos —, seriam necessários 10 policiais especializados permanentemente desdobrados. Os sensores RF-560 e RF-360 da Dedrone operam autonomamente, sem supervisão local, gerenciados por uma equipe centralizada no ComAvE.

3.7.6. Identificação e classificação de ameaças: O documento de especificações do kit DroneShield descreve explicitamente que o RFPatrol deverá indicar a **"possível marca do drone"** por leitura de amplitude de RF. O sistema não realiza decodificação de protocolos; não identifica modelo específico, versão de firmware, protocolo de enlace ou capacidade de carga útil. Drones FPV, DIY e plataformas de campo de batalha não constam de nenhuma base de dados construída exclusivamente por amplitude espectral comercial.

3.7.7. Impossibilidade de distinção friend/foe: Em operação onde drones autorizados da PMMG, CBMMG, Polícia Civil e DECEA voam nas mesmas faixas que drones hostis, a incapacidade de identificar o protocolo específico torna o operador incapaz de distinguir, com confiança técnica, uma ameaça real de uma aeronave amiga. O risco de engajamento equivocado é real e documentável.

3.7.8. Neutralização - Broadband Jamming vs. Protocol Jamming: O DroneGun Tactical opera como jammer de banda larga: emite energia RF simultaneamente nas faixas de 2,4 GHz, 5,8 GHz, 433 MHz, 915 MHz e GNSS, independentemente do protocolo identificado — pois o equipamento não realiza identificação de protocolo. Não há distinção entre modo nominal inteligente e modo de contingência: toda operação com o DroneGun é, por definição, uma operação broadband indiscriminada.

3.7.9. Implicação operacional — Friendly fire eletromagnético: A ativação do DroneGun Tactical em operação urbana da PMMG é operacionalmente comparável ao emprego de munição de efeito de área em zona densamente habitada: qualquer receptor GPS de viatura, rádio tático policial, câmera de vigilância por Wi-Fi ou sistema de comunicação de emergência no raio de atuação será bloqueado. O DedroneDefender 2 não afeta nenhum sistema RF além do canal específico do drone-alvo durante o engajamento.

3.7.10. Implicação regulatória**:** A Resolução ANATEL nº 760/2023 exige que o Bloqueador de Sinais de Radiocomunicações produza interferência estritamente necessária à neutralização da ameaça. O DroneGun Tactical, ao bloquear cinco faixas simultâneas em toda operação, independentemente da ameaça concreta, expõe o órgão contratante a questionamentos de proporcionalidade regulatória em cada acionamento documentado.

3.7.11. Conclusão: O kit DroneShield (RFPatrol + DroneGun Tactical) não atende aos critérios operacionalmente indispensáveis para uma solução C-UAS de nível estadual. As falhas são estruturais — não corrigíveis por configuração, acessórios ou integração com sistemas de terceiros — e afetam os critérios de maior peso operacional: integração da kill chain, seletividade de neutralização, geolocalização do piloto, operação autônoma centralizada e registro forense. O kit está concebido para uso tático militar pontual, não para o modelo de policiamento estadual com gestão centralizada pretendido pela PMMG.

3.7.12. **ANÁLISE TÉCNICA: GoHobby Ltda./Skyfend Technology Co. Ltd. (skyfend Hunter):**

3.7.13. O Skyfend Hunter é comercializado no Brasil pela GoHobby Ltda., empresa distribuidora de drones fundada em 2010, com foco histórico em equipamentos DJI para agricultura de precisão. Sua entrada no segmento C-UAS é recente — os produtos foram lançados em março de 2025. O Skyfend Hunter é fabricado pela Skyfend Technology Co., Ltd., empresa de capital chinês, sem certificações de segurança por agências de países aliados ocidentais (EUA, Reino Unido, UE) equivalentes às que a Dedrone by Axon detém. A GoHobby atua como distribuidora, não como fabricante, detentor de propriedade intelectual ou responsável pelo desenvolvimento da plataforma de segurança.

3.7.14. Arquitetura All-in-One e seus Limites: O Skyfend Hunter integra no mesmo corpo físico as funções de detecção RF, identificação por modelo e jamming adaptativo. Essa arquitetura all-in-one apresenta vantagem de simplicidade operacional de campo — um único equipamento cobre detecção e neutralização — mas impõe teto técnico rígido: todas as etapas da kill chain são limitadas pelos parâmetros físicos de um equipamento handheld com tela de 3,5 polegadas, sem capacidade de expansão modular, sem integração com sensores externos e sem plataforma de C2 que amplie a consciência situacional além do que o operador vê no display.

3.7.15. Implicação operacional — Concepção incompatível com policiamento estadual: O Hunter é projetado para um único operador respondendo a uma ameaça no seu alcance imediato. A solução Dedrone é projetada para um centro de comando que monitora simultaneamente múltiplos pontos do estado, acionando equipes táticas sob demanda. São concepções operacionais fundamentalmente distintas — apenas uma delas é compatível com cobertura territorial estadual permanente.

3.7.16. Implicação operacional — Sem ação policial sobre o piloto**:** O valor mais alto de qualquer sistema C-UAS para a PMMG não é simplesmente detectar um drone — é localizar o operador para captura. O Hunter fornece bearing (direção aproximada) para apontamento do jammer, não coordenadas acionáveis do piloto. A solução Dedrone geolocalizaa tanto o drone quanto o piloto com precisão de 2,5°, fornecendo coordenadas para encaminhamento de equipe terrestre enquanto o engajamento de neutralização está em curso.

3.7.17. Identificação e Classificação de Ameaças: O Skyfend Hunter declara cobertura de hardware de 400 MHz a 6 GHz e base de dados de 'modelos convencionais de UAV'. O número total de modelos cobertos pela biblioteca não é documentado publicamente para o Hunter especificamente. Atualizações da base de dados são realizadas via cabo USB conectado a PC — não há distribuição automática integrada a plataforma de inteligência operacional. Não há documentação de equipe dedicada de SIGINT alimentando a biblioteca com assinaturas de conflitos reais.

3.7.18. Implicação operacional — Cobertura de ameaças não convencionais: 'Modelos convencionais' são, por definição, os drones comerciais mais comuns. Plataformas FPV artesanais, drones com protocolos modificados e equipamentos de fabricação não mainstream são precisamente as ameaças que atores criminosos utilizam para escapar de sistemas de detecção convencionais. A DedroneDNA é alimentada por equipe de SIGINT com acesso a assinaturas de drones em uso em conflitos reais, incluindo modelos não disponíveis comercialmente.

3.7.19. Implicação operacional — Atualização manual dependente de fornecedor chinês: Cada atualização da biblioteca do Hunter requer conexão USB manual por equipamento, com software fornecido pela Skyfend. A capacidade de reconhecer novas ameaças está condicionada ao ritmo de disponibilização pela empresa fabricante e à capacidade técnica local de aplicação. A Dedrone distribui atualizações automaticamente via DedroneTracker.AI para todos os sensores da frota simultaneamente.

3.7.20. Neutralização — Jamming Adaptativo vs. Protocol Jamming por IA: O Skyfend Hunter apresenta capacidade de jamming

adaptativo por modelo: ao detectar um drone, o sistema identifica o modelo e seleciona automaticamente a estratégia de interferência correspondente. Esse comportamento representa evolução real em relação ao jamming broadband puro — em vez de bloquear todas as bandas simultaneamente, o Hunter concentra a interferência na faixa associada ao modelo detectado. Contudo, a arquitetura opera na lógica de cobertura de faixa de frequência por modelo, não de disrupção do protocolo de comunicação específico. O DedroneDefender 2, alimentado pelo DedroneTracker.AI, executa disrupção do protocolo de comunicação exato — não apenas da banda associada ao fabricante — com interferência colateral mínima fora dessa faixa específica.

3.7.21. Conclusão: O Skyfend Hunter apresenta avanços técnicos em relação ao kit DroneShield — notadamente o jamming adaptativo por modelo, maior autonomia de jamming ativo e alcance de neutralização declarado de até 3 km. Esses méritos são reconhecidos. No entanto, o equipamento reproduz as mesmas limitações estruturais que o tornam inadequado para uma operação C-UAS robusta de nível estadual: ausência de integração sistêmica da kill chain, ausência de plataforma de C2, impossibilidade de operação autônoma sem operador local, ausência de geolocalização do piloto para ação policial, cobertura limitada a modelos convencionais sem alimentação por SIGINT operacional, ausência de registro forense estruturado e impossibilidade de escalabilidade territorial sem acréscimo linear de efetivo. A essas limitações técnicas soma-se a questão institucional da origem chinesa do fabricante, sem certificações de segurança equivalentes às detidas pela Dedrone by Axon junto ao Departamento de Segurança Interna dos EUA (DHS SAFETY Act) e ao CPNI/NPSA do Reino Unido — credenciais que atestam que a tecnologia foi auditada por agências governamentais de países aliados para uso em contextos de segurança nacional e pública.

3.7.22. **ANÁLISE TÉCNICA: D-Fend Solutions Ltd. (EnforceAir 2)**

3.7.23. A D-Fend Solutions Ltd. é empresa israelense com escritório nos EUA (Virginia) que desenvolve e comercializa o sistema EnforceAir 2, solução C-UAS baseada em tecnologia de cyber takeover. Diferentemente das demais soluções analisadas, a D-Fend não produz um jammer de radiofrequência — sua tecnologia distintiva é o sequestro cibernético do protocolo de comunicação do drone, assumindo o controle da aeronave e forçando pouso ou retorno ao ponto de origem.

3.7.24. Divergência Fundamental de Tecnologia de Mitigação: A tecnologia de cyber takeover da D-Fend Solutions representa uma abordagem de mitigação legítima e reconhecida no mercado C-UAS global. No entanto, ela é fundamental e irremediavelmente distinta do jamming narrowband protocolo-específico exigido pela necessidade operacional da PMMG.

3.7.25. As diferenças operacionais entre cyber takeover e smart jamming são as seguintes:

Dimensão	Cyber Takeover (D-Fend EnforceAir 2)	Smart Jamming Narrowband (DedroneDefender 2)
Mecanismo de ação	Exploração de vulnerabilidades do protocolo para assumir controle da aeronave	Disrupção narrowband do link de comando e controle no canal de comunicação identificado
Dependência de cobertura do protocolo	Alta — funciona apenas em protocolos com vulnerabilidades conhecidas exploráveis	Independente de vulnerabilidade — atua sobre qualquer protocolo RF identificado
Eficácia contra drones FPV / DIY	Limitada — protocolos customizados não possuem vulnerabilidades catalogadas	Ampla — jamming atua sobre qualquer emissão RF na faixa identificada
Portabilidade (efetor handheld)	NÃO — EnforceAir 2 não possui versão handheld portátil equivalente ao DroneDefender 2	SIM — DedroneDefender 2 handheld com 6,2 kg
Resultado sobre o drone	Controle da aeronave — pouso ou retorno (pode ser desejável em alguns contextos)	Interrupção do link de controle — RTH ou pouso vertical controlado

3.7.26. Constatação técnica determinante**:** A D-Fend Solutions não fabrica um efetor portátil do tipo gun com capacidade de smart jamming narrowband protocolo-específico. O objeto da necessidade administrativa da PMMG exige especificamente essa modalidade de neutralização — não por preferência de marca, mas porque é a única arquitetura compatível com operações urbanas onde a interferência colateral deve ser minimizada e a portabilidade do efetor é operacionalmente indispensável para desdobramento tático em campo. A D-Fend, por não produzir esse tipo de efetor, não pode fornecer o objeto tal como necessário.

3.7.27. Ausência de Presença no Brasil: A D-Fend Solutions não possui representante comercial, distribuidor autorizado, registro de produto no Exército Brasileiro (R-105 / Decreto nº 10.030/2019), homologação ANATEL, nem histórico de contratação pública documentado no Brasil. A ausência de presença nacional configura, de forma independente das limitações técnicas, barreira adicional à viabilidade de contratação para órgão de segurança pública estadual.

3.7.28. Conclusão: A D-Fend Solutions é eliminada da análise de alternativas viáveis por razão técnica determinante: sua tecnologia de mitigação (cyber takeover) é fundamentalmente distinta do smart jamming narrowband portátil exigido pela necessidade administrativa, não sendo substituível, equivalente ou adaptável a esse fim. Trata-se de mismatch de objeto — não de deficiência de desempenho. A D-Fend é uma alternativa para um objeto diferente, não para o objeto desta contratação.

3.7.29. **ANÁLISE TÉCNICA — Dedrone by Axon (Solução de Referência)**

3.7.30. A Dedrone by Axon é empresa americana integrante do grupo Axon Enterprise Inc., fabricante do sistema TASER e maior fornecedor de tecnologia para segurança pública nos Estados Unidos. A Dedrone desenvolve e comercializa plataforma C-UAS integrada composta pelos sensores DedroneSensor RF-560 e RF-360, pelo jammer inteligente DedroneDefender 2 e pela plataforma de comando e

controle DedroneTracker.AI.

3.7.31. A solução está operacional em mais de 1.100 sites globais, incluindo 53 aeroportos internacionais, 64 locais de entretenimento e grandes eventos, 33 instalações governamentais não americanas, 32 entidades federais dos EUA e 6 países membros do G7. A solução é aprovada pelo Departamento de Segurança Interna dos EUA (DHS SAFETY Act — designação QATT) e certificada pelo Centre for the Protection of National Infrastructure do Reino Unido (CPNI/NPSA), sendo a única solução C-UAS com ambas as designações simultaneamente.

3.7.32. Kill-Chain DTI-M — Integração Sistêmica Nativa: A cadeia DTI-M da Dedrone é executada como fluxo automatizado e nativo entre componentes desenvolvidos pelo mesmo fabricante, com protocolos de comunicação proprietários protegidos por patentes. Os sensores RF-560 e RF-360 detectam e classificam o protocolo da ameaça; o DedroneTracker.AI processa os dados via IA/ML e gera o pacote de targeting (protocolo-alvo, bearing de apontamento com precisão de 2,5°, prioridade de engajamento); o DedroneDefender 2 recebe e executa automaticamente a disrupção narrowband no canal correspondente — sem intervenção manual do operador para seleção de protocolo, banda ou frequência. Essa integração sistêmica é protegida por múltiplas patentes registradas, tornando inviável sua replicação por terceiros sem violação de propriedade intelectual.

3.7.33. Biblioteca DedroneDNA — Ativo Proprietário Inimitável: A biblioteca DedroneDNA é o ativo central de inteligência da solução. Ela identifica individualmente cerca de 600 modelos de mais de 150 fabricantes, incluindo protocolos DJI OcuSync, Lightbridge e Enhanced Wi-Fi; Remote ID (padrões americano e europeu); drones FPV; plataformas DIY; e ameaças emergentes documentadas em conflitos armados reais, coletadas por equipe dedicada de inteligência de sinais (SIGINT) atuante em teatros de operações.

3.7.34. As atualizações são distribuídas automaticamente via DedroneTracker.AI para todos os sensores conectados simultaneamente.

3.7.35. A DedroneDNA não é um banco de dados de especificações técnicas públicas — é um ativo proprietário construído ao longo de anos de coleta em ambientes operacionais reais, incluindo conflito ativo. Esse ativo não pode ser replicado por nenhum competidor em prazo compatível com a necessidade administrativa.

3.7.36. DedroneDefender 2 — Protocol Jamming por IA: O DedroneDefender 2 é o único efetor portátil do mercado que combina no mesmo equipamento físico: (a) modo primário de protocol jamming por IA, executado de forma autônoma com base no pacote de targeting gerado pelo DedroneTracker.AI — interferência mínima, restrita ao protocolo do drone-alvo; e (b) modo secundário standalone de contingência, para operação em cenários sem conectividade com a plataforma C2.

3.7.37. Essa combinação de modos em um único equipamento — com o modo primário smart como padrão nominal e o modo secundário como resiliência operacional — é característica arquitetural proprietária da Dedrone, não replicada por nenhum dos competidores analisados.

3.7.38. DedroneTracker.AI — Plataforma C2 de Gestão Centralizada: O DedroneTracker.AI é a plataforma de C2 que unifica toda a operação: detecção em tempo real de múltiplos sensores distribuídos, fusão de sensores RF, câmera PTZ e radar, sistema friend/foe por protocolo, alertas programáveis, geolocalização de drone e piloto em mapa, histórico auditável com cadeia de custódia digital, API REST/MQTT para integração com sistemas governamentais, e suporte a implantação cloud ou on-premises. A plataforma é a base técnica para o modelo de operação remota centralizada que viabiliza a gestão de uma rede de sensores distribuídos pelo estado sem operadores dedicados por ponto.

3.7.39. Capacidades Diferenciadoras Exclusivas

Capacidade	DroneShield	Skyfend Hunter	Dedrone by Axon
Kill chain DTI-M integrada e automatizada por IA	✗	✗	✓
Protocol jamming narrowband por IA (modo primário)	✗	✗	✓
Interferência colateral mínima por protocolo	✗	~	✓
Geolocalização precisa do piloto para ação policial	✗	✗	✓
Sensores autônomos — operação sem operador local	✗	✗	✓
Plataforma C2 cloud com API e friend/foe	✗	✗	✓
Registro forense auditável com cadeia de custódia	✗	✗	✓
Biblioteca SIGINT ≥500 protocolos + battlefield	✗	~	✓
Escalabilidade sem acréscimo de efetivo	✗	✗	✓
DHS SAFETY Act (QATT) — agência G7	✓	✗	✓
CPNI/NPSA (Reino Unido) — segurança nacional	✗	✗	✓

Origem do fabricante — país aliado ocidental	✓ (Austrália/EUA)	✗ **(China)**	✓ (EUA)

3.7.40. Refutação estruturada das demais alternativas

Alternativa	Motivo da Eliminação	Natureza da Falha
DroneShield (RFPatrol + DroneGun Tactical)	Broadband jamming indiscriminado; kill chain desintegrada; ausência de plataforma C2; geolocalização de piloto inoperante; sem registro forense; incompatível com ambiente urbano.	Falha estrutural — não corrigível por configuração ou integração com terceiros.
GoHobby / Skyfend Hunter	Jamming adaptativo por banda, não por protocolo; sem C2 integrado; sem geolocalização de piloto; base de dados limitada a modelos convencionais; origem chinesa sem certificação de segurança ocidental; sem registro forense; presença no mercado de apenas 12 meses.	Falha estrutural em critérios indispensáveis + questão de segurança institucional.
D-Fend Solutions (EnforceAir 2)	Tecnologia de cyber takeover — categoricamente distinta do smart jamming narrowband portátil exigido. Não produz efetor handheld do tipo gun. Sem presença no Brasil.	Incompatibilidade de objeto — fornece tecnologia de mitigação de categoria diferente.
Integração de componentes de fabricantes distintos	A integração de sensores de um fabricante com jammer de outro elimina a capacidade de smart jamming autônomo — que depende de protocolo de comunicação nativo entre sensor, C2 e efetor. A automaticidade da seleção de protocolo, latência zero e targeting por bearing são capacidades da integração nativa, não replicáveis por API genérica entre produtos heterogêneos.	Inviabilidade técnica de composição: a função central do objeto — smart jamming autônomo — depende de integração nativa proprietária.

4. DETALHAMENTO DA SOLUÇÃO ESCOLHIDA

4.1. **Descrição da solução como um todo (PREENCHIMENTO OBRIGATÓRIO)** ***(art. 6º, VII, da Resolução Seplag nº 115, de 2021)***

4.2. **Componente 1: Sensor RF de longo alcance com decodificação**

4.2.1. O sensor RF de longo alcance constitui o componente primário de detecção da solução. Deverá ser fornecido equipamento novo, em sua versão mais recente, com todos os acessórios necessários para operação imediata.

4.2.2. **Tipo de operação e princípio de funcionamento.** O sensor deverá operar exclusivamente em modo passivo, realizando apenas a recepção e análise de sinais de radiofrequência emitidos por drones e seus controles remotos. O equipamento não deverá emitir sinais RF para fins de detecção, dispensando autorização da ANATEL para transmissão e não introduzindo interferência no ambiente eletromagnético, o que assegura operação discreta e compatível com atividades de inteligência e investigação policial.

4.2.3. **Alcance de detecção.** O sensor deverá apresentar alcance mínimo de detecção de 5 km (cinco quilômetros) em condições típicas, quando operado com antenas omnidirecionais para cobertura de 360° (trezentos e sessenta graus). Quando operado com antenas direcionais para cobertura de 180° (cento e oitenta graus), o alcance mínimo deverá ser de 8 km (oito quilômetros) em condições típicas. Os alcances consideram linha de visada entre o sensor e o drone em condições normais de ambiente eletromagnético. O alcance elevado é indispensável para garantir tempo de reação adequado na proteção de grandes perímetros e para viabilizar a cobertura de áreas extensas com menor número de sensores.

4.2.4. **Tecnologia de detecção e faixas de frequência.** O sensor deverá utilizar tecnologia de Rádio Definido por Software (SDR — Software Defined Radio) com múltiplos scanners de frequência integrados, operando nas faixas de 2,4 GHz, 5,2 GHz e 5,8 GHz, no mínimo. A tecnologia SDR permite varredura simultânea em ampla faixa espectral, reduzindo o tempo de detecção e conferindo adaptabilidade a novos protocolos por meio de atualizações de software, sem substituição de hardware.

4.2.5. **Classificação e biblioteca proprietária de assinaturas.** O sensor deverá realizar a classificação dos drones detectados por meio de comparação das assinaturas RF captadas com biblioteca proprietária de assinaturas de drones mantida pelo fabricante. A biblioteca deverá conter, no momento do fornecimento, no mínimo, 200 (duzentos) protocolos distintos, cobrindo, no mínimo, 600 (seiscentos) modelos de drones de pelo menos 150 (cento e cinquenta) fabricantes diferentes. A cobertura deverá abranger protocolos de drones comerciais, drones FPV (First Person View), drones DIY (construção artesanal) e drones de campo de batalha emergentes. A classificação é indispensável para a priorização de ameaças e para a habilitação do smart jamming protocolo-específico pelo efetor de mitigação integrado.

4.2.6. **Atualização da biblioteca.** A biblioteca de assinaturas deverá ser atualizada remotamente via plataforma C2 em nuvem, com periodicidade mínima trimestral durante o período de garantia, sem necessidade de intervenção presencial junto ao sensor. A atualização remota é indispensável diante da evolução constante do cenário de ameaças, com novos modelos de drones e protocolos surgindo continuamente.

4.2.7. **Radiogoniometria e geolocalização.** O sensor deverá ser capaz de determinar o azimute da origem do sinal RF detectado por meio de técnica de Ângulo de Chegada (AoA — Angle of Arrival). Adicionalmente, o sensor deverá suportar geolocalização por Diferença de Tempo de Chegada (TDoA — Time Difference of Arrival), sem necessidade de hardware adicional, proporcionando precisão superior na localização do drone e do piloto. A geolocalização deverá ser possível por triangulação com 2 (duas) ou mais unidades de sensores, plotando automaticamente a posição do drone e do piloto no mapa georreferenciado da plataforma C2. A capacidade de geolocalização do piloto, e não apenas do drone, é indispensável para a interceptação policial e a persecução penal.

4.2.8. **Configuração de antenas.** O sensor deverá ser fornecido com configuração flexível de antenas, incluindo antenas omnidirecionais para cobertura de 360° e antenas direcionais para cobertura de 180° com alcance estendido. Ambas as configurações deverão ser fornecidas com o equipamento, permitindo alternância conforme o cenário operacional, sem necessidade de ferramentas especiais. A flexibilidade de configuração de antenas permite adaptar o sensor a cenários distintos — cobertura ampla de perímetro ou vigilância direcional de longo alcance — sem aquisição de equipamentos adicionais.

4.2.9. **Conectividade e integração.** O sensor deverá possuir GPS integrado para georreferenciamento automático e conectividade Ethernet (conector RJ45) para conexão à infraestrutura de tecnologia da informação local. O equipamento deverá ser apto à conexão nativa com a plataforma C2 em nuvem. A configuração, a operação e os alarmes do sensor deverão ser realizados integralmente por meio da interface web da plataforma C2. As atualizações de firmware e da biblioteca de assinaturas deverão ser realizadas remotamente via plataforma C2. A conectividade nativa em nuvem com GPS integrado é o que viabiliza a instalação rápida em cenários móveis, sem infraestrutura prévia de rede.

4.2.10. **Recepção de Remote ID.** O sensor deverá ser capaz de receber e processar sinais de Remote ID conforme os padrões internacionais vigentes, incluindo, no mínimo: Wi-Fi Beacon, Wi-Fi NAN (Neighbor Awareness Networking), Bluetooth 4 e Bluetooth 5. O processamento de Remote ID permite a correlação dos dados de detecção com informações regulatórias do drone, possibilitando a distinção entre aeronaves registradas e não registradas.

4.2.11. **Ambiente operacional.** O sensor deverá ser projetado e otimizado para operação em ambientes urbanos com alta densidade de sinais de radiofrequência (RF-noisy), minimizando falsos positivos decorrentes de interferências de estações-base de telecomunicações, redes Wi-Fi, dispositivos Bluetooth e demais emissores presentes em centros urbanos.

4.2.12. **Características físicas e ambientais.** O sensor deverá atender às seguintes especificações: dimensões máximas de 384 mm × 194 mm × 690 mm (L × P × A); peso máximo de 10,0 kg (dez quilogramas) com antenas e suporte de montagem; grau de proteção mínimo IP65, assegurando proteção total contra poeira e jatos de água; faixa de temperatura operacional de -10°C a +55°C; alimentação CA 100-240 V 50/60 Hz e/ou PoE, garantindo flexibilidade de instalação. As dimensões e o peso reduzidos são indispensáveis para viabilizar o transporte e a montagem em configuração de kit móvel.

4.2.13. **Integração nativa.** O sensor deverá ser nativamente compatível com a plataforma C2 e com o efetor de mitigação portátil do mesmo ecossistema, assegurando fusão de sensores com latência mínima e habilitação do smart jamming protocolo-específico. Não serão aceitos sensores que requeiram integração por middleware ou interfaces de programação de aplicações genéricas para comunicação com a plataforma C2 ou com o efetor.

4.3. **Componente 2: Sensor RF compacto com radiogoniometria**

4.3.1. O sensor RF compacto com radiogoniometria complementa o sensor primário de longo alcance, proporcionando capacidade de determinação de direção por Ângulo de Chegada (AoA) para geolocalização precisa de drones e pilotos por triangulação. Suas dimensões e peso reduzidos permitem transporte e montagem por operador único.

4.3.2. **Tipo de operação e cobertura.** O sensor deverá operar exclusivamente em modo passivo, com cobertura omnidirecional de 360° e radiogoniometria integrada por AoA. O equipamento não deverá emitir sinais de radiofrequência para fins de detecção, dispensando autorização da ANATEL e mantendo a discrição operacional.

4.3.3. **Alcance de detecção.** O sensor deverá apresentar alcance mínimo de detecção de 2 km (dois quilômetros) para a maioria dos drones em condições normais, podendo atingir até 5 km (cinco quilômetros) em condições ideais para drones específicos. O alcance é adequado para proteção de perímetros de eventos e infraestruturas, complementando o sensor de longo alcance na rede de sensores distribuídos.

4.3.4. **Precisão da radiogoniometria.** A acurácia da radiogoniometria deverá ser de, no máximo, ±5° (cinco graus) de erro médio, assegurando precisão mínima para que a triangulação com 2 ou mais sensores produza geolocalização operacionalmente útil.

4.3.5. **Geolocalização.** O sensor deverá realizar geolocalização de drones e pilotos por triangulação com 2 ou mais unidades, inclusive de pilotos que operem drones por enlaces Wi-Fi. A posição do drone e do piloto deverá ser plotada automaticamente no mapa georreferenciado da plataforma C2. A capacidade de geolocalizar pilotos via Wi-Fi é relevante porque parcela significativa dos drones de menor porte opera por esse protocolo.

4.3.6. **Características físicas.** O sensor deverá atender às seguintes especificações: dimensões máximas de 300 mm × 300 mm × 450 mm (L × P × A); peso máximo de 8,0 kg (oito quilogramas), viabilizando transporte e montagem por operador único; grau de proteção mínimo IP65; faixa de temperatura operacional de -10°C a +55°C. As dimensões compactas são indispensáveis para a configuração de kit móvel portátil.

4.3.7. **Conectividade e integração.** O sensor deverá possuir terminal satelital e/ou roteador LTE e GPS integrados, bem como conectividade Ethernet, sendo apto à conexão nativa com a plataforma C2 em nuvem. A instalação rápida deverá ser viabilizada pela conectividade integrada, sem necessidade de infraestrutura de rede prévia. As atualizações de firmware e da biblioteca de assinaturas deverão ser realizadas remotamente via plataforma C2. O sensor deverá ser nativamente compatível com a plataforma C2 e com o sensor de longo alcance do mesmo ecossistema, assegurando fusão de dados sem latência adicional.

4.3.8. **Alimentação.** O sensor deverá suportar alimentação por PoE IEEE 802.3bt (60W) para operação em rede cabeada, ou CA 100-240 V 50/60 Hz. A dupla opção de alimentação garante flexibilidade para diferentes cenários de desdobramento.

4.3.9. **Ambiente operacional.** O sensor deverá ser otimizado para operação em ambientes urbanos com alta densidade de sinais RF (RF-noisy), minimizando falsos positivos em centros urbanos.

4.3.10. **Montagem.** O sensor deverá ser compatível com montagem em mastro com diâmetro entre 40 mm e 90 mm, por meio de suporte incluído no fornecimento, e com montagem em tripé de campo. A versatilidade de montagem permite instalação tanto em configuração portátil (tripé) quanto em configurações semifixas (mastro em edificação).

4.4. **Componente 3: Efetor de mitigação inteligente portátil (smart jammer)**

4.4.1. O efetor de mitigação inteligente portátil constitui o componente de mitigação da solução, operando primariamente como terminal inteligente do ecossistema integrado. Sua função é neutralizar drones detectados e classificados pela cadeia de sensores, por meio de disrupção protocolo-específica dos enlaces de comando, controle, vídeo e navegação GNSS do drone-alvo.

4.4.2. **Fator de forma e ergonomia.** O equipamento deverá possuir formato handheld do tipo gun (rifle ou pistola), com empunhadura dupla, permitindo apontamento direcional rápido e preciso pelo operador. O peso máximo, incluindo bateria, deverá ser de 7,0 kg (sete quilogramas), assegurando ergonomia para uso prolongado em operação tática. Não serão aceitos equipamentos no formato mochila (backpack), em razão da limitação de apontamento direcional inerente a esse formato.

4.4.3. **Modo primário de operação — conectado/smart.** O modo primário e nominal de operação deverá ser o modo conectado, no qual o equipamento opera como terminal inteligente da plataforma C2 em nuvem. Neste modo, a plataforma C2 processa os dados de classificação dos sensores RF, aplica algoritmos de inteligência artificial e aprendizado de máquina para priorização por risco e gera o pacote de targeting, que é transmitido em tempo real ao jammer, contendo o protocolo exato a ser disruptado, o azimute de apontamento e a prioridade de engajamento. O jammer executa automaticamente a disrupção narrowband exclusivamente na faixa de frequência correspondente ao protocolo identificado, com seleção autônoma e sem intervenção manual do operador para escolha de banda ou protocolo. Este modo é indispensável para o modelo operacional pretendido pelo ComAvE e constitui a capacidade central que distingue a solução de alternativas broadband.

4.4.4. **Bandas de frequência e modos de disrupção.** O equipamento deverá cobrir as bandas ISM (2,4 GHz; 5,8 GHz; 900/868 MHz; 433 MHz) e GNSS (GPS L1, L2 e L5; BeiDou B1 e B3; Galileo E5b), no mínimo. O equipamento deverá realizar:

a) disrupção de controle remoto — disrupção narrowband protocolo-específica de enlaces de comando, controle e vídeo em múltiplas bandas, com mínima interferência colateral em faixa e fora de faixa;

b) disrupção GNSS — disrupção de sinal de satélite para desabilitação de navegação autônoma do drone.

4.4.5. A cobertura de bandas ISM e GNSS multi-constelação/multi-banda é indispensável porque os drones modernos utilizam receptores que operam simultaneamente em múltiplas constelações e frequências de navegação.

4.4.6. **Cone efetivo.** O ângulo do cone efetivo de disrupção deverá ser de, no máximo, 25° (vinte e cinco graus), com cone de targeting de 20° (vinte graus). A concentração de energia em cone estreito maximiza o alcance efetivo na direção da ameaça e minimiza a interferência colateral em direções adjacentes, requisito indispensável para operação em ambiente urbano.

4.4.7. **Tempos de ativação.** O tempo de partida a frio para jamming em banda (broadband emergencial) deverá ser inferior a 1 (um) segundo. O tempo de partida a frio para jamming protocolo-específico (smart jamming) deverá ser de, no máximo, 10 (dez) segundos. Esses tempos asseguram capacidade de reação rápida tanto em modo emergencial quanto em modo nominal.

4.4.8. **Autonomia e alimentação.** O equipamento deverá possuir autonomia mínima de 30 (trinta) minutos de operação contínua, correspondente ao turno operacional mínimo de um engajamento tático. A alimentação deverá ser por bateria militar removível e recarregável do tipo AN/PRC-148 ou equivalente.

4.4.9. **Display de targeting.** O equipamento deverá possuir display ou aplicativo de targeting integrado que apresente, em tempo real, informações de azimute de apontamento provenientes da plataforma C2 em nuvem, permitindo que o operador engaje ameaças mesmo quando o drone estiver além da linha de visada (BVLOS — Beyond Visual Line of Sight). O display deverá combinar a indicação de azimute com o cone de targeting do equipamento. Esta capacidade é indispensável para o modelo operacional do ComAvE, no qual a equipe tática é acionada remotamente e pode chegar ao ponto de ameaça sem visão direta do drone.

4.4.10. **Capacidade anti-swarm.** O equipamento deverá ser capaz de neutralizar múltiplos drones simultaneamente, utilizando capacidades combinadas de jamming protocolo-específico e disrupção GNSS, conforme coordenação da plataforma C2 para sequenciamento de protocolos-alvo. O cenário de múltiplos drones simultâneos é ameaça crescente, particularmente relevante em operações sobre presídios e ataques a infraestruturas críticas.

4.4.11. **Conformidade militar e ambiental.** O equipamento deverá atender à norma MIL-STD-810H para robustez em operação tática, incluindo resistência a choques, vibração, temperatura, umidade, altitude e chuva. O grau de proteção deverá ser, no mínimo, IP65. A faixa de temperatura operacional deverá ser de -10°C a +55°C.

4.4.12. **Vedação: detecção embarcada.** Não serão aceitos equipamentos que possuam sistema de detecção RF embarcado no próprio jammer. Esta vedação decorre de limitações técnicas incontornáveis: alcance de detecção inferior a 500 m, insuficiente para tempo de reação; falsos positivos por autointerferência do sinal de jamming nos circuitos de recepção; impossibilidade física de detecção passiva simultânea ao jamming ativo na mesma faixa de frequência; e ausência de capacidade de geolocalização precisa, que requer triangulação com múltiplos sensores separados espacialmente.

4.4.13. **Vedação: broadband exclusivo.** Não serão aceitos equipamentos que operem exclusivamente em modo broadband, sem capacidade de jamming protocolo-específico (smart jamming). A operação exclusivamente broadband é inadequada para ambiente urbano por causar interferência generalizada em sistemas de comunicação circundantes, incluindo redes celulares, Wi-Fi e, criticamente, sistemas de comunicação de emergência (SAMU, Bombeiros e Polícia).

4.4.14. **Modo secundário de operação — standalone/contingência.** O equipamento deverá possuir, adicionalmente, capacidade de operação em modo standalone, sem conexão com a plataforma C2 ou internet, como modo de contingência para cenários excepcionais de perda de conectividade. Neste modo, o operador seleciona manualmente as bandas de mitigação. As capacidades do modo standalone são inferiores ao modo primário, incluindo perda de seletividade protocolo-específica, perda de targeting por azimute, perda de coordenação anti-swarm inteligente e perda de registro forense centralizado. O modo standalone não substitui nem equivale ao modo conectado — constitui recurso secundário para garantir capacidade residual de mitigação.

4.4.15. **Integração nativa com plataforma C2.** A integração entre o jammer e a plataforma C2 deverá ser bidirecional e nativa, utilizando protocolos de comunicação proprietários do ecossistema. O jammer deverá ser nativamente compatível com a plataforma C2 e com os sensores RF do mesmo ecossistema, assegurando smart jamming autônomo protocolo-específico e targeting em tempo real. Não serão aceitos jammers que dependam de integração por middleware ou interfaces de programação de aplicações genéricas para comunicação com a C2 ou com os sensores.

4.4.16. A proposta comercial deverá ser composta ainda de licenciamento integrado de software. O fornecimento do Kit objeto deste Item 01 compreenderá, de forma integrada e indissociável ao fornecimento do hardware, o licenciamento de uso do firmware residente nos sensores dos Componentes 1A e 1B e o licenciamento dos respectivos módulos de software desses sensores na plataforma C2 objeto do Item 02, pelo período de 60 (sessenta) meses. Não será admitido o fornecimento do hardware dos sensores dissociado do licenciamento de software necessário à sua operação plena.

4.4.17. O Kit deverá incluir caixas de transporte robustas, em material polimérico de alta resistência ou equivalente, com grau de proteção mínimo IP65 quando fechadas, conforme norma IEC 60529, e elementos de mobilidade integrados contemplando rodízios e alças. As caixas deverão acondicionar os respectivos sensores, antenas, suportes, baterias, cabos de alimentação e dados pré-conectorizados de fábrica e demais elementos auxiliares necessários à operação.

4.4.18. O kit deverá conter 1 (um) terminal de comunicação satelital em órbita terrestre baixa (LEO — Low Earth Orbit), integrado de fábrica ao Kit, viabilizando a conectividade dos sensores dos Componentes 1A e 1B com a plataforma de Comando e Controle em nuvem do licenciamento integrado de software, sem necessidade de infraestrutura prévia de rede no local de desdobramento. O terminal satelital deverá ser homologado pela Agência Nacional de Telecomunicações (ANATEL) para operação no território brasileiro.

4.4.19. O terminal satelital deverá ser fornecido como subsistema completo, contendo, no mínimo, a antena satelital LEO dimensionada para cobertura plena no território brasileiro, o cabo de alimentação dedicado, os cabos Ethernet de interconexão com os sensores do Kit, o switch de rede Ethernet com capacidade compatível com o tráfego simultâneo dos sensores e do terminal, e as instruções operacionais de campo em língua portuguesa do Brasil.

4.5. **Justificativas para o parcelamento ou não da solução (PREENCHIMENTO OBRIGATÓRIO)** ***(art. 6º, VIII, da Resolução Seplag nº 115, de 2021)***

4.5.1. A decisão acerca do parcelamento deve observar, de forma motivada, a viabilidade técnica e a vantajosidade econômica da divisão do objeto. As orientações do TCU registram que o parcelamento pode ser afastado quando descaracteriza ou prejudica o objeto, quando se mostra necessário preservar a padronização, quando provoca aumento dos custos globais ou quando os benefícios potenciais da divisão não compensam o acréscimo das dificuldades administrativas de gestão contratual. No mesmo sentido, o TCU ressalta que a definição do objeto e dos requisitos da contratação deve ser precisa, suficiente e clara, sem especificações excessivas, desnecessárias ou irrelevantes, mas preservando os elementos efetivamente necessários ao adequado atendimento da necessidade administrativa.

4.5.2. No caso concreto, a contratação não tem por objeto a aquisição isolada de equipamentos autônomos e intercambiáveis, mas sim uma solução C-UAS móvel/portátil integrada, cuja utilidade operacional depende do funcionamento coordenado e nativo entre sensores RF, biblioteca proprietária de assinaturas, plataforma de comando e controle em nuvem, lógica de classificação e priorização, recursos de direcionamento de engajamento, efetor portátil de mitigação, registro forense, atualização centralizada e suporte evolutivo. Trata-se, portanto, de solução considerada como um todo, e não de simples agregação de bens independentes. A divisão do objeto comprometeria a própria identidade funcional da contratação.

4.5.3. Indivisibilidade funcional da cadeia operacional: O não parcelamento justifica-se, em primeiro lugar, pela indivisibilidade funcional da cadeia operacional pretendida. O núcleo da necessidade administrativa está na cadeia automatizada em que o sensor detecta e classifica o protocolo, a C2 processa e prioriza o evento, e o efetor executa a mitigação protocolo-específica correspondente. Se esses elementos forem contratados separadamente, a Administração passará a depender de camadas adicionais de integração, tradução de dados, compatibilização de versões, validação cruzada e desenvolvimento sob medida, o que descaracteriza a solução definida no planejamento e compromete o desempenho exigido. Nesse cenário, não haveria mero parcelamento do fornecimento, mas modificação substancial da solução técnica necessária.

4.5.4. Interoperabilidade nativa, propriedade intelectual e unidade tecnológica: Também é inviável o parcelamento porque a interoperabilidade crítica entre sensores, C2, biblioteca e efetor é nativa e protegida por propriedade intelectual, inserida em ecossistema único, com protocolos proprietários, autenticação entre componentes, formato unificado de dados e atualização coordenada. A contratação fracionada exigiria tentativa de recompor artificialmente, por múltiplos contratos, uma arquitetura cuja efetividade depende justamente de sua unidade tecnológica. Quando a padronização e a coerência arquitetural são indispensáveis ao objeto, o afastamento do parcelamento encontra amparo na própria lógica admitida pelo TCU.

4.5.5. Latência mínima da cadeia de decisão: Há, ainda, razão operacional decisiva relacionada à latência mínima da cadeia de decisão. Em ambiente C-UAS, o tempo entre detecção, classificação, decisão, direcionamento de engajamento e mitigação constitui fator crítico de sucesso. Cada interface adicional entre fabricantes distintos tende a ampliar a latência, o risco de incompatibilidade semântica, a perda de parâmetros, a inconsistência de versões e as falhas de disponibilidade. Em missões dinâmicas de segurança pública, especialmente diante de drones rápidos, múltiplos ou de curta janela de reação, a redução da latência não representa conveniência, mas requisito operacional essencial. A divisão do objeto, nesse contexto, comprometeria a aptidão da solução para cumprir a finalidade pública que justifica a contratação.

4.5.6. Segurança operacional e prevenção de fratricídio eletrônico: O parcelamento também se revela incompatível com a segurança operacional e a prevenção de fratricídio eletrônico. A classificação friend/foe, as listas de autorização, as regras automáticas de alerta, a priorização por risco e o acionamento do efetor precisam estar inseridos no mesmo ambiente lógico e decisório. Em solução fracionada, cresce o risco de divergência entre classificação, direcionamento de engajamento e resposta, inclusive com possibilidade de neutralização indevida de aeronaves autorizadas ou de emissão inadequada em área urbana sensível. Em objeto mission-critical, a preservação da unidade entre sensoriamento, classificação e ação constitui elemento necessário ao adequado atendimento da necessidade administrativa.

4.5.7. Integridade forense e cadeia de custódia digital: Outro fundamento relevante reside na integridade forense e na cadeia de custódia digital. A solução pretendida deve registrar, de forma automática, íntegra e auditável, o ciclo completo do evento, inclusive classificação, posição do drone e do piloto, alertas, decisões, direcionamento de engajamento, mitigação e resultado do engajamento. Em contratação parcelada, cada subsistema tenderia a gerar registros próprios, com formatos, temporalidades, granularidade e lógicas

distintas, fragilizando a reconstrução confiável do evento e reduzindo a utilidade probatória dos dados. Considerando que a necessidade administrativa envolve não apenas resposta operacional, mas também inteligência, responsabilização e produção de prova, a integridade informacional da solução unitária é requisito central e não pode ser tratada como acessório.

4.5.8. Segurança cibernética e governança tecnológica: A fragmentação do objeto amplia, ainda, a superfície de ataque cibernético e dificulta a governança tecnológica. Múltiplos fornecedores significam mais interfaces expostas, mais conectores, mais credenciais, mais fronteiras entre sistemas, mais pontos de falha e maior complexidade na aplicação coordenada de patches, atualizações e medidas de contenção de incidentes. Para solução sensível de comando, sensoriamento e mitigação, a arquitetura unificada reduz risco técnico, simplifica a governança e favorece maior controle sobre segurança, disponibilidade e integridade dos dados. Exigências compatíveis com a natureza e a relevância do objeto são admitidas pelo TCU justamente para assegurar seu satisfatório cumprimento.

4.5.9. Gestão unificada em nuvem: Além disso, o modelo operacional pretendido pressupõe gestão unificada em nuvem de sensores distribuídos, biblioteca de assinaturas, regras de alerta, analytics, notificações, logs e pacotes de direcionamento de engajamento. Em ecossistemas proprietários, não se pode presumir que componentes de fabricantes distintos se conectem à mesma instância em nuvem com equivalência funcional plena. Em regra, a fragmentação conduz à multiplicação de plataformas paralelas ou a integrações ad hoc, ambas incompatíveis com a operação remota centralizada pretendida. Nessa hipótese, o parcelamento prejudica a solução como um todo e, por isso, deve ser rejeitado.

4.5.10. Integridade do ciclo de smart jamming protocolo-específico: No ponto mais sensível da contratação, o parcelamento comprometeria a integridade do ciclo de smart jamming protocolo-específico. Essa capacidade depende da correspondência exata entre protocolo identificado, lógica de direcionamento de engajamento e emissão narrowband correspondente. Cada etapa adicional de tradução entre subsistemas heterogêneos representa novo ponto de falha: erro de mapeamento, incompatibilidade de versões, perda de parâmetros, aumento de latência e degradação da precisão do engajamento. Em termos práticos, a divisão do objeto converteria o modo nominal integrado em modo degradado, aproximando a solução de modelos broadband ou standalone, justamente aquilo que o planejamento identificou como insuficiente para o atendimento da necessidade pública.

4.5.11. Padronização, escalabilidade e preservação do investimento público: O parcelamento também se mostra inadequado sob o ponto de vista da padronização, da escalabilidade e da preservação do investimento público. A contratação não se limita ao kit portátil inicial; ela deve permitir expansão futura para novas unidades sensoras, conversão para arranjos semifixos, fixos ou veiculares e crescimento da malha de monitoramento sem ruptura arquitetural. A fragmentação contratual transferiria à Administração o ônus permanente de compatibilizar subsistemas heterogêneos, elevando o risco de obsolescência, perda de padronização, custos de integração e eventual necessidade de substituição integral da arquitetura no médio prazo. O TCU admite o não parcelamento quando necessário à padronização ou quando a divisão compromete a utilidade do objeto.

4.5.12. Ressalte-se, por fim, que o não parcelamento não decorre de preferência por marca, fabricante ou modelo, nem representa restrição artificial à competitividade. Ao contrário, decorre da conclusão técnica de que a necessidade administrativa somente pode ser adequadamente atendida por solução unitária, integrada e coerente com os requisitos definidos no planejamento. O TCU veda especificações excessivas, desnecessárias ou irrelevantes que limitem indevidamente a competição; porém, admite e exige a preservação dos requisitos que sejam efetivamente necessários ao satisfatório cumprimento do objeto. Assim, eventual redução do universo de fornecedores não resulta de escolha arbitrária da Administração, mas da própria complexidade e indivisibilidade funcional da solução requerida. Em outras palavras, não se está restringindo indevidamente a competição; está-se apenas reconhecendo, de forma motivada e tecnicamente demonstrada, os limites reais do mercado diante do objeto definido.

4.5.13. Por fim, visando ampliar a competitividade, bem como pela possibilidade de adquirir os sensores de forma isolada para operação de monitoramento, principalmente de forma descentralizada, a administração optou por dividir o processo em 02 lotes distintos, quais sejam:

LOTE	ITENS	CÓDIGO DO ITEM NO SIAD	DESCRIÇÃO DO ITEM CATMAS	UNIDADE DE AQUISIÇÃO	QUANTIDADE
01	ITEM 01	2039273	KIT ANTI-DRONE - APLICACAO: PROTECAO ANTIAEREA CONTRA DRONES; DISTANCIA DE DETECCAO: MINIMO 5KM (OMNIDIRECIONAL) E 8KM (DIRECIONAIS); FREQUENCIA DE OPERACAO: MULTIBANDA ISM (MINIMO 2.4 GHZ E 5.8 GHZ); INTERFACE DE COMUNICACAO: POR SINAL; DIMENSOES: COMPACTO (FIXAR EM MASTROS, TRIPES OU VIATURAS); PESO: UNIDADE SENSORA INFERIOR A 6 KG; BATERIA: (POE/AC/DC) OU BATERIA RECARREGAVEL; ACESSORIOS: SUPORTE FIXACAO, CABO DE REDE/ENERGIA, ANTENA;	UNIDADE	03

	ITEM 02	2039281	KIT ANTI-DRONE - APLICACAO: PROTECAO ANTIAEREA CONTRA DRONES; DISTANCIA DE DETECCAO: MINIMO DE 1 KM A 2 KM (EM LINHA DE VISADA); FREQUENCIA DE OPERACAO: MULTIBANDA, GNSS/GPS, 2.4 GHZ E 5.8 GHZ; INTERFACE DE COMUNICACAO: SINAL; DIMENSOES: PORTATIL E ERGONOMICO PARA USO TATICO; PESO: INFERIOR A 7,5 KG (COM BATERIAS ACOPLADAS); BATERIA: ION-LITIO RECARREGAVEL, AUTONOMIA MINIMA 25 MIN; ACESSORIOS: CARREGADOR,BATERIA , MALETA TRANSPORTE, BANDOLEIRA;	UNIDADE	03
02	ITEM 01	2039273	KIT ANTI-DRONE - APLICACAO: PROTECAO ANTIAEREA CONTRA DRONES; DISTANCIA DE DETECCAO: MINIMO 5KM (OMNIDIRECIONAL) E 8KM (DIRECIONAIS); FREQUENCIA DE OPERACAO: MULTIBANDA ISM (MINIMO 2.4 GHZ E 5.8 GHZ); INTERFACE DE COMUNICACAO: POR SINAL; DIMENSOES: COMPACTO (FIXAR EM MASTROS, TRIPES OU VIATURAS); PESO: UNIDADE SENSORA INFERIOR A 6 KG; BATERIA: (POE/AC/DC) OU BATERIA RECARREGAVEL; ACESSORIOS: SUPORTE FIXACAO, CABO DE REDE/ENERGIA, ANTENA;	UNIDADE	03

4.5.14. Dessa forma a administração buscar adquirir não somente os sensores que sejam compatíveis com o JAMMER, mas também sensores que tenham operacionalidade de forma dissociada.

4.6. **Contratações correlatas ou interdependentes *(art. 6º, XI, da Resolução Seplag nº 115, de 2021)***

4.6.1. Em pesquisas no PNCP - Portal Nacional de contratações públicas foi verificado que recentemente o STF - Supremo tribunal Federal adquiriu por inexigibilidade de licitação sistema similar ao que pretende-se adquirir. É o que se extrai do documento 135582735 acostado ao presente processo:

SUPREMO TRIBUNAL FEDERAL

CONTRATO N. 50/2025

CONTRATO DE AQUISIÇÃO DE SISTEMA ANTIDRONE, QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO SUPREMO TRIBUNAL FEDERAL, E A EMPRESA AXON ENTERPRISE INC POR INTERMÉDIO DA ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA. (Dispensa de licitação - Processo Administrativo Eletrônico n. 000152/2025)

A **UNIÃO**, por intermédio do **SUPREMO TRIBUNAL FEDERAL,** sediado na Praça dos Três Poderes, em Brasília - Distrito Federal, CNPJ 00.531.640/0001-28, neste ato representado por sua Diretora-Geral Adjunta, Senhora **Fernanda do Valle Azambuja**, no uso das atribuições que lhe confere o Regulamento da Secretaria do Supremo Tribunal Federal, doravante denominado **CONTRATANTE**, e a empresa **AXON ENTERPRISE INC,** sociedade empresária estrangeira, regularmente constituída sob as leis do Estado do Arizona, Estados Unidos da América, com sede na 17800 N 85th Street, Scottsdale, Arizona, 85255, inscrita no Employer Identification Number (EIN) sob nº 86-0741227, por intermédio da **ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA,** CNPJ/MF nº 03.232.670/0001-21, com sede na Avenida Copacabana, nº 325, Barueri/SP, CEP 06472-001, neste ato representada por seu sócio, Sr. **Rafael Alves de Souza**, doravante denominada **CONTRATADA**, celebram o presente Contrato, com fundamento na Lei n. 14.133/2021, observando-se as normas constantes na Lei Complementar n. 123/2006, o contido no Processo Administrativo Eletrônico n. 000152/2025 e em conformidade com as disposições a seguir.

DO OBJETO

CLÁUSULA PRIMEIRA – O objeto do presente Contrato é a aquisição de sistema antidrone, observados o Termo de Referência (Anexo II deste Contrato) e a proposta da **CONTRATADA** (Anexo I deste Contrato), os quais, independentemente de transcrição, são partes integrantes deste instrumento, naquilo que não o contrarie.

4.6.2. A diferença principal reside no fato de que o sistema adquirido pelo STF é FIXO conformidade necessidade demonstrada pelo órgão.

4.6.3. Conforme exaustivamente apresentado no presente ETP, o sistema FIXO não atende às necessidades da PMMG/COMAVE em virtude do dinamismo que envolve a atividade policial. Todavia a contratação correlata apresentada é suficiente para comprovar que a "tecnologia antidrone" é uma realidade inegável e crescente no cenário nacional.

4.6.4. Já a Polícia Federal assinou **ata de registro de preços** 135582735 para aquisição de "fuzil jammer", mas, conforme

justificado no item 3.6.12 o "jammer" de forma isolada não atende aos anseios da PMMG/COMAVE para o contexto operacional no qual se insere.

POLÍCIA FEDERAL
SCN Q. 4, 3º Andar, Bloco C, Ed. Multibrasil Corporate - Edifício-Sede da Polícia Federal, , Brasília/DF, CEP 70297-400
Telefone: (61) 2024-8115 - http://www.pf.gov.br

MJSP - POLÍCIA FEDERAL
ATA DE REGISTRO DE PREÇOS
Nº 03-2025 CGAD/DLOG

Processo nº 08200.001993/2024-78

A POLÍCIA FEDERAL, por intermédio da COORDENAÇÃO GERAL DE ADMINISTRAÇÃO (CGAD/DLOG/PF) UASG 200334, com sede no Setor Comercial Norte, Quadra 04, do Edifí. Multibrasil Corporate, Asa Norte, Brasília-DF, 70714-903, inscrito(a) no CNPJ/MF sob o nº 00.394.494/0014-50, neste ato representado pelo Delegado de Polícia Federal ANDRÉ LUIS LIMA CARMO, Ordenador de Despesas, nomeado pela Portaria nº 17.389-DG/PF, de 23 de janeiro de 2023, publicada no Boletim de Serviço nº 017, de 24 de janeiro de 2023, portador da matrícula funcional nº 1542699, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS Nº 90022/2024, conforme consta no documento Termo de Homologação (39750850), processo administrativo nº 08200.001993/2024-78, RESOLVE registrar os preços da empresa indicada e qualificada nesta ATA, de acordo com a classificação por ela alcançada e nas quantidades cotadas, atendendo as condições previstas no edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. **DO OBJETO**

1.1. A presente Ata tem por objeto o registro de preços para a eventual aquisição de Sistema de Proteção Contra Drones (C-UAS: Counter Uncrewed Aerial Systems), especificados no item 3 do Termo de Referência, anexo I do Edital de Licitação nº 14/2024, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2. **DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS**

2.1. O preço registrado, as especificações do objeto, as quantidades de cada item, fornecedores e as demais condições ofertadas nas propostas são as que seguem:

FORNECEDOR: GOHOBBY FUTURE TECHNOLOGY LTDA. **CNPJ**: nº 13.373.898/0001-95
ENDEREÇO: Av. Marginal Projetada, 1652, Galpão 11, Sala 14, Tamboré, Barueri, SP **CEP**: 06460-200

REPRESENTANTE: VANESSA VIEIRA PAREDES **CPF:** 413.656.508-98 **RG:** 39.735.717-5 SSP-SP
ENDEREÇO: Av. Engenheiro Luís Carlos Berrini, 105, Conj. 605, Cidade Monções, Cidade: São Paulo UF: SP **CEP:** 04.571-900
FONE: (11) 5103-2333 Ramal: 111, (11) 91444-3434 **E- MAIL**: licitacao@gohobby.com.br

ITEM	DESCRIÇÃO	MARCA/MODELO	QUANTIDADE HOMOLOGADA	VALOR UNITÁRIO	VALOR TOTAL
3	Fuzil Jammer AntiDrone (Rádio transceptor, tipo portátil, potência 2 w, quantidade canais 6 un, freqüência modulação vhs-152 a 161 mhz e uhf-458 a 470 m, alcance máximo 3.000 m, fonte alimentação bateria recarregável, características adicionais clip fixação cinto, acessórios carregador de bateria rápido 110/220 v)	Fabricante/ Marca: SKYFEND Modelo: SkyFend - Hunter SHH100 ou similar	11	R$ 383.000,00	R$ 4.213.000,00
				VALOR TOTAL	R$ 4.213.000,00

4.7. **Resultados pretendidos *(art. 6º, IX, da Resolução Seplag nº 115, de 2021)***

4.7.1. Como resultado da contratação, espera-se que o órgão demandante passe a dispor de capacidade operacional móvel, escalável e efetivamente utilizável em campo para prevenção, detecção, acompanhamento, identificação e resposta a ocorrências envolvendo Aeronaves Remotamente Pilotadas (ARP), em apoio direto às operações da Polícia Militar.

4.7.2. A contratação deverá produzir, de forma cumulativa, os seguintes resultados esperados:

Ampliação da consciência situacional aérea em operações policiais: incremento da capacidade institucional de perceber, em tempo oportuno, a presença de aeronaves remotamente pilotadas em áreas de interesse operacional, inclusive em cenários dinâmicos, urbanos, conflagrados ou de elevada sensibilidade tática.

Redução do tempo de resposta a ameaças aéreas não autorizadas: diminuição do intervalo entre a detecção do evento, sua qualificação operacional, a disseminação da informação ao comando e o acionamento das equipes responsáveis pela resposta, favorecendo atuação mais célere, coordenada e eficaz.

Aumento da capacidade de proteção de efetivos, autoridades, instalações e áreas sensíveis: fortalecimento das condições de segurança em operações policiais, grandes eventos, missões especiais, ações em estabelecimentos sensíveis, proteção de dignitários e outras situações em que a presença de drones represente risco à integridade de pessoas, ao êxito da missão ou à continuidade de serviços essenciais.

Melhoria da capacidade de atuação em campo em face de ameaças tecnicamente diversas: aptidão institucional para lidar não apenas com drones comerciais amplamente difundidos, mas também com plataformas FPV, sistemas DIY, aeronaves adaptadas e outros perfis emergentes de ameaça, compatibilizando a resposta estatal com a evolução tecnológica observada no ambiente operacional contemporâneo.

Apoio qualificado à tomada de decisão pelo comando: disponibilização, em tempo real, de informações técnicas e operacionais relevantes ao centro de comando, inclusive alertas, trilhas de evento, azimute, dados de localização relativa e demais elementos úteis à coordenação da resposta, ao gerenciamento do risco e à alocação racional dos meios disponíveis.

Maior efetividade das equipes táticas de campo: aumento da capacidade de emprego orientado das frações responsáveis pela intervenção, com deslocamento mais preciso ao ponto de interesse, melhor compreensão da ameaça em curso e maior probabilidade de êxito na contenção do evento, na abordagem dos envolvidos e na preservação da segurança da operação.

Apoio à localização do operador remoto e à responsabilização dos agentes envolvidos: geração de elementos operacionais aptos a subsidiar a identificação e localização do ponto de controle da aeronave, favorecendo a atuação policial voltada à interceptação, abordagem, investigação e responsabilização administrativa, civil ou penal dos autores.

Geração e preservação de registros para fins operacionais, de inteligência e de prova: produção automática e estruturada de históricos, alarmes, registros de eventos, metadados e demais registros associados às ocorrências, em padrão que permita sua utilização em análise posterior, aprendizado institucional, produção de conhecimento de inteligência e eventual instrução probatória.

Racionalização do emprego de efetivo especializado: adoção de modelo operacional que permita monitoramento

centralizado e operação remota de sensores distribuídos, reduzindo a necessidade de manter operador técnico presencial em cada ponto de detecção e viabilizando melhor aproveitamento do efetivo especializado disponível.

Viabilização de expansão progressiva e escalável da capacidade estadual: criação de base tecnológica e operacional apta a permitir a ampliação gradual da cobertura, inicialmente em configuração móvel/portátil e, conforme a evolução da maturidade institucional, também em arranjos semifixos ou fixos, sem necessidade de reformulação estrutural do modelo de comando e operação.

Padronização doutrinária e procedimental do enfrentamento à ameaça UAS: estabelecimento de ambiente mais favorável à consolidação de protocolos operacionais, fluxos de acionamento, critérios de resposta, rotinas de monitoramento e procedimentos de coordenação entre comando, aviação, inteligência e equipes de campo.

Redução de vulnerabilidades operacionais diante do uso criminoso de drones: mitigação do risco associado ao emprego de aeronaves remotamente pilotadas por organizações criminosas para monitoramento de ações policiais, transporte de ilícitos, reconhecimento aéreo, apoio logístico, perturbação de operações e outras condutas hostis.

Elevação da capacidade institucional de pronta resposta em contexto móvel: disponibilidade de solução apta a ser rapidamente desdobrada em operações temporárias, contingenciais, itinerantes ou emergenciais, sem dependência de infraestrutura prévia complexa, ampliando a flexibilidade de emprego da Polícia Militar em todo o território estadual.

Fortalecimento da eficiência administrativa e do interesse público envolvido: obtenção de capacidade operacional compatível com o risco contemporâneo, com melhor relação entre cobertura, mobilidade, centralização do comando e aproveitamento de recursos humanos e materiais, em benefício da segurança pública e da proteção de ativos estratégicos do Estado.

4.7.3. Em síntese, espera-se que a contratação resulte na efetiva estruturação de capacidade operacional móvel de enfrentamento a ameaças representadas por drones, integrada ao ciclo decisório da Polícia Militar, apta a apoiar o comando, orientar as equipes em campo, ampliar a proteção de ambientes sensíveis e permitir expansão progressiva da cobertura operacional em âmbito estadual.

4.8. **Providências a serem adotadas *(art. 6º, X, da Resolução Seplag nº 115, de 2021)***

4.8.1. Para a viabilização da solução e a regular instrução do processo, deverão ser adotadas as seguintes providências:

4.8.1.1. **Elaboração do Termo de Referência** contendo todas as descrições técnicas dos bens que pretende-se adquirir;

4.8.1.2. **Instruir** o processo com todos os demais documentos necessários ao lançamento do pregão eletrônico internacional com fulcro na Lei Federal nº 14.133/2021;

4.8.1.3. **Publicidade e Formalização:** Adotar as providências administrativas necessárias para garantir a ampla publicidade da contratação;

4.8.1.4. **Logística de Recebimento:** Preparação do hangar do COMAVE para o recebimento dos equipamentos e designação de militares capacitados para a conferência técnica e recebimento dos mesmos;

4.8.1.5. **Gestão de Capacitação:** Programação de datas e designação do efetivo que passará pelo treinamento técnico-operacional junto aos especialistas da empresa contratada;

4.8.1.6. **Designar formalmente a comissão de militares especialistas do Esquadrão HARPIA** que figurarão como equipe de fiscalização da contratação;

4.9. **Possíveis impactos ambientais *(art. 6º, XII, da Resolução Seplag nº 115, de 2021)***

4.9.1. Não resulta em emissão de poluentes, não envolve intervenção, modificação ou supressão de bens ambientais em ecossistemas, biomas ou áreas de preservação, tampouco produz rejeito ou lixo que deva ter tratamento especializado. As pilhas/baterias esgotadas e que não forem mais reutilizáveis excepcionalmente utilizadas para alimentação dos componentes, quando inviável à operação, serão descartadas conforme normas em vigor referentes ao descarte deste tipo de material.

5. POSICIONAMENTO CONCLUSIVO (PREENCHIMENTO OBRIGATÓRIO) *(ART. 6º, XIII, DA RESOLUÇÃO SEPLAG Nº 115, DE 2021)*

5.1. Diante das minuciosas ponderações elaboradas no presente Estudo Técnico Preliminar, conclui-se de maneira segura que a adoção da aquisição do **sistema integrado de detecção, rastreamento e mitigação de ARP** por meio de pregão eletrônico nos termos da Lei Federal nº 14.133/2021 é a via administrativa correta, necessária e mais favorável para responder aos desafios atuais de segurança mapeados pela Polícia Militar de Minas Gerais, contemplando na sua integralidade o interesse público e institucional.

5.2. Esta deliberação assenta-se em robustas justificativas técnicas, operacionais e financeiras. Na prática das operações diárias, as unidades de segurança pública necessitam intervir imediatamente diante das inovações táticas adotadas pela criminalidade organizada, sob pena de perda de vidas e quebra da ordem pública. Tecnicamente, a aquisição destes sistemas de contramedida eletrônica insere o Estado em um patamar de modernidade e garantia operacional ímpar.

ASSINATURAS:

Documento assinado eletronicamente por **Rodrigo Bertini Glória**, **1º Tenente**, em 24/04/2026, às 22:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

Documento assinado eletronicamente por **Tony Carlo Souza Silva**, **Capitão**, em 25/04/2026, às 22:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

Documento assinado eletronicamente por **DANIEL AUGUSTO DOS SANTOS SILVA**, **Agente de Contratação**, em 26/04/2026, às 12:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017 .

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **135562813** e o código CRC **54E49A02**.

Referência: Processo nº 1250.01.0005266/2026-49 SEI nº 135562813