



TOMADA DE SUBSÍDIO	
Edital Nº 1078/2025	Objeto Embarque Seguro
ANEXO I – OPORTUNIDADE E CONTRIBUIÇÕES ESPERADAS	

## 1. OPORTUNIDADE DE NEGÓCIO

- 1.1 A presente tomada de subsídio tem como objetivo coletar informações e contribuições do mercado para subsidiar a modelagem de uma parceria estratégica que visa o desenvolvimento conjunto de uma solução tecnológica avançada e escalável, voltada à Administração Pública.
- 1.2 Uma **Oportunidade de Negócio** consiste na identificação de uma demanda concreta por parte de uma entidade pública ou privada que, ao ser compartilhada com o SERPRO, possibilita o desenvolvimento conjunto de uma nova solução tecnológica ou a evolução de uma solução existente. Essa iniciativa deve estar orientada à geração de valor público, com foco na oferta do produto ou serviço a órgãos da Administração Pública nas esferas federal, estadual ou municipal.
- 1.3 A caracterização de uma oportunidade ocorre, em regra, a partir da constatação de uma dor, necessidade ou problema real que afeta a atuação de agentes públicos e cuja superação demanda inovação, integração tecnológica, maior eficiência ou segurança. É fundamental que o SERPRO tenha participação efetiva na concepção, construção e entrega da solução, agregando sua capacidade técnica, sua infraestrutura tecnológica e sua legitimidade institucional como empresa pública federal.
- 1.4 A solução proposta (**Embarque Seguro**) tem como objetivo estruturar e ofertar uma plataforma tecnológica de autenticação biométrica e controle de acesso baseada em reconhecimento facial, aplicável a diversos modais de transporte — incluindo aéreo, metroferroviário, rodoviário e hidroviário — bem como a ambientes de grande circulação de pessoas, como portos, terminais, estádios, centros de convenções e demais espaços com requisitos críticos de segurança, rastreabilidade ou automação do fluxo de acesso.
- 1.5 A proposta contempla uma solução ponta a ponta, que abrangerá desde o pré-cadastro e manifestação de consentimento do usuário até a autenticação biométrica em tempo real nos pontos físicos de controle. O modelo operacional deverá prever a disponibilização em ambiente de nuvem segura, com suporte à interoperabilidade com sistemas de terceiros, capacidade de operação offline, gestão de consentimento, registros auditáveis e aderência integral às normas legais e regulatórias vigentes, inclusive em matéria de proteção de dados pessoais.
- 1.6 Para a viabilizar e ofertar essa solução, o SERPRO buscará a formação de parcerias estratégicas com o setor privado, por meio do instrumento de Parceria em Oportunidade de Negócio (PON), nos termos do Art. 28 da Lei nº 13.303/2016, com o objetivo de compor arranjos que integrem competências tecnológicas, fornecimento de infraestrutura e equipamentos, integração de sistemas e prestação de serviços especializados, garantindo escalabilidade, segurança e excelência operacional na entrega da solução.

- 
- 1.7 Entre os benefícios esperados, destacam-se a adoção de uma solução integrada de validação biométrica para aprimorar significativamente os mecanismos de segurança pública e nacional, ao permitir a identificação positiva, segura e automatizada de indivíduos em pontos críticos de acesso. A autenticação biométrica baseada em reconhecimento facial, aliada ao cruzamento com bases oficiais e auditáveis, mitigaria riscos associados ao uso de documentos falsos ou cartões de acesso indevidos. Com isso, ampliaria a capacidade de prevenir fraudes, identificar pessoas procuradas ou envolvidas em ilícitos e asseguraria maior controle sobre o fluxo de indivíduos em ambientes sensíveis.
- 1.8 Do ponto de vista operacional, a plataforma contribuirá para o aumento da eficiência nos processos de controle de acesso e embarque. Ao automatizar etapas hoje manuais — como conferência de documentos e validação de bilhetes — a solução reduziria filas, tempos de espera e a dependência de mão de obra presencial. Isso iria se traduzir em maior capacidade de atendimento, otimização do uso de posições físicas de controle e diminuição de atrasos operacionais, com impactos positivos sobre o planejamento e a logística dos operadores envolvidos.
- 1.9 Em termos de experiência do usuário, a solução proporcionará uma jornada mais fluida, segura e desburocratizada. A eliminação da necessidade de apresentação de documentos físicos, o embarque sem contato e a possibilidade de pré-cadastro remoto garantiriam maior comodidade e agilidade ao cidadão, além de ampliar o tempo disponível para a fruição de serviços e produtos oferecidos nos terminais, impactando positivamente as receitas acessórias dos operadores.
- 1.10 Do ponto de vista institucional e regulatório, a solução deverá ser desenhada com observância integral à legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), e deverá contar com trilhas de auditoria, gestão de consentimento, segregação de ambientes, conformidade de segurança da informação e mecanismos de resposta a incidentes. A oferta em ambiente de nuvem com escalabilidade controlada, capacidade de operação em contingência (offline) e interoperabilidade com sistemas legados e de terceiros deverá assegurar também a aderência a requisitos técnicos e operacionais demandados por diferentes perfis de clientes públicos e privados.
- 1.11 Por fim, a centralização dos dados operacionais em dashboards e painéis analíticos — com indicadores de fluxo, desempenho e ocupação — possibilitará uma gestão mais eficiente dos ambientes atendidos, subsidiando o planejamento tático e estratégico de operadores, gestores públicos e órgãos de segurança. Ao unificar diferentes modalidades e pontos de controle sob uma mesma lógica de autenticação biométrica, a solução contribuirá para a padronização nacional de tecnologias de acesso seguro, com ganhos em interoperabilidade, rastreabilidade e governança.

---

## **2. CONTRIBUIÇÕES ESPERADAS**

---

2.1 Para a construção do conhecimento que visa auxiliar na modelagem da parceria em oportunidade de negócio, espera-se o recebimento de contribuições relacionadas às questões a seguir:

### **2.2 Modalidades de Transporte e Ambientes de Grande Circulação**

---

---

2.2.1 Quais modais de transporte (aéreo, rodoviário, ferroviário, hidroviário, metroviário) podem se beneficiar da solução proposta?

2.2.2 Quais modais atualmente apresentam maior maturidade tecnológica para implantação da solução proposta?

2.2.3 Em cidades com múltiplos modais integrados, existe viabilidade técnica e operacional para adoção da solução proposta?

2.2.4 A solução proposta pode ser aplicada ao controle de acesso em ambientes de grande circulação, como estádios, arenas, feiras, centros de convenções e parques temáticos?

2.2.5 Há casos concretos de interoperabilidade entre operadores de diferentes modais, com compartilhamento de dados de embarque validados biometricamente?

## **2.3 Equipamentos Necessários**

2.3.1 Quais são os principais equipamentos de hardware envolvidos na solução proposta (*e-gates*, catracas, câmeras, sensores, totens etc.)?

2.3.2 Existem equipamentos certificados e aptos para uso em ambientes externos e sujeitos a intempéries?

2.3.3 Terminais de autoatendimento (como totens) são comumente utilizados na experiência de embarque com biometria?

2.3.4 Existem *e-gates* ou catracas já integradas com sistemas de validação biométrica facial?

2.3.5 Quais são os requisitos mínimos de hardware para garantir operação em alta disponibilidade?

2.3.6 Existe padronização técnica ou normativa para equipamentos de biometria no Brasil?

2.3.7 Os equipamentos utilizados precisam ser homologados por entidades reguladoras (ex: ANAC, ANTT, INMETRO)?

2.3.8 Em caso de falha de rede, é necessário que haja infraestrutura de contingência local?

2.3.9 Quais tecnologias de detecção de prova de vida ("*liveness detection*") são usualmente embarcadas nesses equipamentos?

## **2.4 Software e Integração**

2.4.1 Qual é o papel do software de biometria facial na solução proposta?

---

2.4.2 Quais APIs ou padrões de integração são mais utilizados para conectar a solução a sistemas legados dos operadores?

2.4.3 É necessária integração com plataformas públicas, como Gov.br, SISBRAIP ou bancos de dados governamentais?

2.4.4 O software de biometria deve estar homologado por algum órgão específico?

2.4.5 A solução permite operação em modo offline, com sincronização posterior dos dados?

2.4.6 O sistema utiliza base própria de biometria facial ou depende de integração com bases de terceiros (governo, parceiros)?

2.4.7 Quais linguagens ou padrões tecnológicos são comumente utilizados nas integrações com os sistemas dos modais?

2.4.8 A solução dispõe de painel de monitoramento centralizado para visualização em tempo real?

2.4.9 A solução contempla funcionalidades de gestão de fluxo e controle de ocupação?

2.4.10 A solução registra logs auditáveis e atende integralmente às exigências da LGPD?

## **2.5 Infraestrutura em Nuvem**

2.5.1 A solução é compatível com operação em nuvem pública, privada ou híbrida?

2.5.2 A empresa possui experiência em projetos de biometria facial operando 100% em ambiente de nuvem?

2.5.3 Quais são os requisitos mínimos de infraestrutura para hospedagem da solução em nuvem?

2.5.4 A solução foi concebida com arquitetura nativa em nuvem ("*cloud native*") ou foi migrada posteriormente ("*lift and shift*")?

2.5.5 A arquitetura faz uso de contêineres, orquestração com *Kubernetes* ou tecnologias *serverless*?

2.5.6 Existe elasticidade automática para lidar com picos de demanda (ex: feriados, eventos)?

2.5.7 Como é feita a segregação lógica e física dos dados dos diferentes operadores em ambientes *multi-tenant*?

2.5.8 A solução segue princípios de segurança como Zero Trust, criptografia ponta a ponta e gestão de identidade federada?

2.5.9 O sistema permite rastreabilidade total de acessos e operações realizadas na nuvem?

---

2.5.10 Existem limitações legais ou operacionais para hospedagem dos dados exclusivamente em território nacional?

## **2.6 Perfil dos Fornecedores e Modelos de Entrega**

2.6.1 Empresas fornecedoras dessa solução costumam atuar como integradoras de sistemas, desenvolvedoras de software, fabricantes de hardware ou operadoras do serviço?

2.6.2 A entrega da solução costuma ser feita diretamente pelo desenvolvedor do software ou por parceiros integradores?

2.6.3 É comum que a solução seja fornecida por empresas que atuam em toda a cadeia (hardware, software, operação)?

2.6.4 Existe presença relevante de startups especializadas nesse mercado?

2.6.5 É comum que o modelo de entrega envolva consórcios entre empresas com competências complementares?

2.6.6 Fabricantes de hardware (câmeras, catracas, *e-gates*) também oferecem o software embarcado ou a operação do sistema?

2.6.7 Há predominância de soluções oferecidas por empresas de tecnologia da informação, segurança eletrônica ou automação?

2.6.8 Existem empresas atuando exclusivamente no fornecimento do software biométrico facial, sem envolvimento com operação?

2.6.9 É comum a atuação de operadores terceirizados responsáveis pela gestão e manutenção do sistema após a implantação?

2.6.10 O modelo *white-label* é uma prática comum entre fornecedores dessa solução?

## **2.7 Capacidade Técnica e Escalabilidade**

2.7.1 As empresas fornecedoras possuem estrutura operacional e técnica para atender demandas em âmbito nacional?

2.7.2 Quais estratégias são adotadas para escalar a solução em grandes hubs de passageiros, como aeroportos internacionais ou terminais rodoviários?

2.7.3 Há experiência na implantação da solução em ambientes de alta complexidade e movimentação, como estações metropolitanas e intermodais?

---

2.7.4 Existem operadores especializados em implantações de grande porte com atuação recorrente no Brasil?

2.7.5 Qual o tempo médio necessário para implantação da solução em um terminal de porte médio?

2.7.6 Quão pode ser escalada para atender eventos temporários e de grande público, como festas populares, shows, competições esportivas ou eleições?

2.7.8 O modelo de solução permite operação simultânea em múltiplos modais e operadores distintos

2.7.9 Qual é a vida útil média dos equipamentos utilizados na solução, considerando as condições de operação contínua?

2.7.10 A empresa possui estrutura técnica para prover suporte contínuo em escala nacional, inclusive em regiões remotas?

## **2.8 Segurança, LGPD e Governança**

2.8.1 Quais medidas são adotadas para garantir a proteção dos dados pessoais sensíveis, como as informações biométricas dos passageiros?

2.8.2 A solução implementa criptografia dos dados em repouso e em trânsito?

2.8.3 Há mecanismos de segregação lógica e física dos dados por operador, terminal ou região?

2.8.4 O processo de embarque com biometria envolve o consentimento explícito do passageiro? Como esse consentimento é registrado?

2.8.5 A solução prevê interfaces seguras para compartilhamento de informações com autoridades públicas (ex: Polícia Federal, ANAC, ANTT)?

2.8.6 Os dados biométricos são armazenados localmente, em nuvem privada ou referenciados em bases públicas federais?

2.8.7 A empresa possui certificações relacionadas à segurança da informação, como ISO 27001, NIST, LGPD Compliance ou equivalentes?

2.8.8 O sistema possui mecanismos de redundância geográfica e recuperação de desastres?

2.8.9 Toda ação no sistema (validação, acesso, falha, recusa) é registrada em trilha de auditoria com carimbo de data/hora?

2.8.10 Em caso de incidente de segurança ou violação de dados, qual é o plano de resposta adotado e em quanto tempo ele é executado?

---

## 2.9 Regulação e Normas Setoriais

- 2.9.1 Quais normas técnicas e regulatórias se aplicam ao uso de validação biométrica para fins de embarque em transportes no Brasil?
- 2.9.2 A solução precisa estar em conformidade com regulações da ANAC, ANTT, ANTAQ, metrô ou agências reguladoras estaduais/municipais?
- 2.9.3 Quais são os principais entraves ou desafios regulatórios atualmente enfrentados na implantação dessa solução?
- 2.9.4 A biometria pode substituir integralmente a apresentação de documentos físicos (ex: RG, CNH, bilhete de embarque)?
- 2.9.5 Existe alguma regulamentação vigente que proíba ou restrinja o uso de biometria facial para embarque em determinados modais?
- 2.9.6 Os modais brasileiros possuem normas específicas para controle de acesso biométrico (portarias, resoluções etc.)?
- 2.9.7 Como é tratada a responsabilização legal em caso de erro na identificação biométrica (ex: falsa rejeição ou aceitação)?
- 2.9.8 Leis municipais ou estaduais impõem restrições ao uso de biometria em transportes públicos ou eventos?
- 2.9.9 É necessário obter anuência formal de agências reguladoras ou entes públicos para implantação da solução em cada modal?
- 2.9.10 A solução já foi submetida à avaliação ou *sandbox* regulatório em algum ente da administração pública?

## 2.10 Modelos de Comercialização

- 2.10.1 Quais são os modelos de negócio mais recorrentes para fornecimento da solução (compra direta, *leasing*, SaaS, BPO)?
- 2.10.2 Há práticas de cobrança por transação (modelo "pay-per-use") no uso da validação biométrica por passageiro ou por acesso?
- 2.10.3 Como normalmente se estrutura a remuneração dos fornecedores em contratos com operadores privados de transporte?
- 2.10.4 Os custos da solução costumam ser arcados integralmente pelo operador ou há possibilidade de cofinanciamento público?

---

2.10.5 Há modelos de parceria em que a solução é implantada por terceiros com pagamento baseado em desempenho (modelo PPP ou concessão)?

2.10.6 Existe margem financeira para oferta da solução por meio de concessionárias ou permissionárias de serviços públicos?

2.10.7 Modelos comerciais baseados em economia de escala (volume alto, custo unitário menor) são aplicáveis à solução?

2.10.8 A precificação dos equipamentos e *software* é afetada diretamente por variações cambiais?

2.10.9 Existe variação significativa de precificação por tipo de modal atendido (aéreo, rodoviário, metroviário etc.)?

2.10.10 É possível contratar a solução por tempo limitado ou de forma sob demanda, como em eventos de curta duração?

## **2.11 Casos Práticos, Experiência e Relacionamento com o Setor Público**

2.11.1 A empresa já implantou soluções de controle de acesso com validação biométrica em ambientes reais no Brasil?

2.11.2 Em quais modais ou ambientes (ex: aeroportos, rodoviárias, arenas, fronteiras, etc.) as soluções já foram utilizadas?

2.11.3 A empresa possui contratos vigentes ou já executados com órgãos da Administração Pública (federal, estadual ou municipal) para esse tipo de solução?

2.11.4 Os contratos firmados com o setor público envolveram fornecimento de solução completa ou apenas parte da tecnologia (software, equipamentos, integração, etc.)?

2.11.5 A empresa participou de licitações, chamamentos públicos ou parcerias com entes estatais para fornecer soluções de biometria?

2.11.6 Quais aprendizados técnicos ou operacionais foram extraídos de experiências anteriores com o setor público?

2.11.7 Foram implantados projetos-piloto ou provas de conceito com órgãos públicos? Quais foram os resultados obtidos?

2.11.8 Houve aumento comprovado de eficiência ou segurança nos projetos implantados com validação biométrica?

---

2.11.9 A empresa possui indicadores ou métricas sobre tempo médio de atendimento, redução de filas ou ganho de produtividade?

2.11.10 Quais falhas técnicas, operacionais ou de aceitação do usuário foram identificadas em implantações anteriores?

2.11.11 Em projetos anteriores, foi necessária campanha de comunicação ou orientação ao público para adoção da biometria?

2.11.12 O sistema implantado foi bem aceito por públicos diversos como idosos, pessoas com deficiência (PcD), crianças e estrangeiros?

2.11.13 Há dados consolidados sobre taxas de falsa rejeição e falsa aceitação nos projetos já realizados?

2.11.14 A empresa participou de projetos com integração internacional (companhias aéreas estrangeiras, sistemas internacionais de segurança, etc.)?

2.11.15 Existe conhecimento prático da empresa sobre normas, regulamentações e requisitos específicos de órgãos públicos para esse tipo de tecnologia?

## **2.12 Ambientes em Nuvem e Infraestrutura Tecnológica**

2.12.1 A solução proposta pode operar em nuvem pública, privada ou híbrida?

2.12.2 Há alguma restrição quanto à localização da infraestrutura de nuvem (território nacional vs. internacional)?

2.12.3 A empresa possui parceria com provedores de nuvem governamental ou certificações para atuar nesse ambiente?

2.12.4 O sistema pode ser hospedado em infraestrutura do contratante, como datacenter próprio ou nuvem estatal?

2.12.5 Há suporte à integração via APIs *RESTful* com sistemas legados de entes públicos?

2.12.6 A infraestrutura da solução atende requisitos de alta disponibilidade (HA) e escalabilidade automática?

2.12.7 Existem modelos com operação 100% remota e centralizada, sem necessidade de servidores locais nos pontos de controle?

2.12.8 A empresa possui arquitetura de microserviços, contêineres (Docker) ou orquestração (*Kubernetes*)?

---

2.12.9 A solução permite operação “edge computing”, com processamento local em caso de falha de rede?

2.12.10 É possível operar o sistema com múltiplos níveis de redundância e disaster recovery automatizado?

### **2.13 Aplicabilidade em Ambientes de Alta Circulação**

2.13.1 A solução pode ser adaptada para controle de acesso em ambientes de grande circulação, como estádios, arenas esportivas, shows e centros de convenções?

2.13.2 Já houve aplicação da tecnologia em eventos temporários com grande fluxo de público?

2.13.3 A solução é compatível com normas de evacuação de emergência e controle de multidões?

2.13.4 O sistema pode operar de forma integrada com catracas, torniquetes ou portões de segurança?

2.13.5 Há alguma limitação quanto à iluminação, movimentação rápida ou cobertura parcial do rosto?

2.13.6 A solução permite identificar comportamentos suspeitos ou padrões de aglomeração via videomonitoramento?

2.13.7 Existe módulo de *analytics* embarcado para análise em tempo real de dados de acesso?

2.13.8 A solução permite operação de múltiplos pontos de entrada simultaneamente, com sincronização?

2.13.9 É possível operar o sistema com dispositivos móveis, como tablets e smartphones dos fiscais?

2.13.10 Há recursos de personalização do fluxo de entrada conforme tipo de evento ou perfil do público?

### **2.14 Inovações Tecnológicas e Inteligência Artificial**

2.14.1 A solução possui recursos de IA embarcada, como reconhecimento facial com aprendizado contínuo (machine learning)?

2.14.2 A IA da solução é treinável com base no perfil do local ou características demográficas da população atendida?

2.14.3 Há mecanismos de detecção de tentativas de fraude (ex: apresentação de foto, máscara ou vídeo)?

2.14.4 A solução permite análise comportamental para predição de riscos ou comportamentos anômalos?

---

2.14.5 Existem dashboards inteligentes com indicadores operacionais em tempo real?

2.14.6 A IA pode operar em ambiente offline com posterior sincronização?

2.14.7 Há funcionalidades de classificação de filas, grupos prioritários ou inteligência de fluxo de passageiros?

2.14.8 O sistema é capaz de operar com múltiplas câmeras simultaneamente para mesma pessoa (fusão de imagens)?

2.14.9 A solução conta com recurso de autoaprendizado em ambientes multiculturais ou com diversidade étnica?

2.14.10 O sistema pode gerar insights para tomada de decisão estratégica dos operadores?

## **2.15 Inclusão, Acessibilidade e Diversidade**

2.15.1 A solução foi testada para diferentes tipos de rosto, tons de pele, características faciais e gênero?

2.15.2 Quais mecanismos foram adotados para garantir acurácia na identificação de pessoas negras, indígenas, orientais, etc.?

2.15.3 O sistema é acessível a pessoas com deficiência visual, auditiva ou mobilidade reduzida?

2.15.4 A interface do usuário permite operação assistida ou comando por voz?

2.15.5 Há documentação em formatos acessíveis, como audiodescrição ou leitura automática?

2.15.6 A solução atende às diretrizes internacionais de acessibilidade digital (WCAG, W3C, etc.)?

2.15.7 Foram realizados testes com público 60+ (idosos) e qual foi a taxa de aceitação e acerto?

2.15.8 Crianças podem ser identificadas com o mesmo nível de acurácia? Há limite de idade mínimo recomendado?

2.15.9 Como é tratado o consentimento de uso da biometria no caso de menores ou pessoas tuteladas?

2.15.10 Há modo alternativo de autenticação caso a biometria falhe?

## **2.16 Cenário Pós-Pandemia e Segurança Sanitária**

2.16.1 A solução pode ser adaptada para controle de temperatura corporal por câmera termográfica?

2.16.2 Já foram implantados dispositivos para identificação de febre ou sintomas visuais durante pandemias?

- 
- 2.16.3 O sistema suporta análise de uso de máscara facial como critério de acesso?
- 2.16.4 Existem mecanismos de distanciamento automático entre passageiros durante o processo de validação?
- 2.16.5 Os dispositivos são sem contato físico? Há risco de contaminação por toque em tela ou sensor?
- 2.16.6 A solução pode integrar-se com sistemas de passaporte vacinal ou certificados sanitários?
- 2.16.7 Há histórico de uso da solução durante a COVID-19 ou outras crises sanitárias?
- 2.16.8 Quais adaptações foram feitas no hardware ou software para atender esse tipo de cenário?
- 2.16.9 O sistema pode se adaptar rapidamente a novas regras de biossegurança ou pandemia futura?
- 2.16.10A tecnologia pode contribuir para um ambiente mais seguro e monitorado em terminais públicos?

## **2.17 Integração Internacional, Geopolítica e Interoperabilidade**

- 2.17.1 A solução é compatível com bases internacionais de dados biométricos (ex: ICAO, Interpol, SITA)?
- 2.17.2 Já houve integração com companhias aéreas estrangeiras ou operadores multinacionais?
- 2.17.3 A tecnologia foi exportada ou adaptada para outros países?
- 2.17.4 A empresa já implantou soluções em aeroportos, terminais ou eventos no exterior?
- 2.17.5 A empresa observa políticas de soberania nacional de dados?
- 2.17.6 A empresa já enfrentou questões geopolíticas relacionadas ao uso da biometria em países com sanções ou restrições?
- 2.17.7 A solução permite interoperabilidade com sistemas de segurança de fronteira e imigração?
- 2.17.8 A empresa possui representação ou alianças internacionais para expandir o uso da tecnologia?
- 2.17.9 O sistema está preparado para operar em múltiplos idiomas?
- 2.17.10 Há planos ou pilotos para uso da solução em integração sul-americana (Mercosul, etc.)?