

---

**ANEXO I – OPORTUNIDADE E CONTRIBUIÇÕES ESPERADAS****Edital Nº  
1341/2025****Objeto  
Conecta Cidades****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 destinada ao desenvolvimento conjunto de uma solução tecnológica integrada, interoperável e escalável, voltada à gestão inteligente de operações urbanas, segurança pública, mobilidade e serviços ao cidadão, no âmbito da Administração Pública.

**1.2** Uma Oportunidade de Negócio consiste na identificação de uma demanda concreta de um ente público ou parceiro privado que, ao ser compartilhada com o SERPRO, oportuniza a concepção e o desenvolvimento conjunto de uma nova solução tecnológica ou o aprimoramento de uma já existente. A iniciativa deve gerar valor público mensurável, privilegiando a transformação digital de serviços e a ampliação da capacidade de gestão e de atendimento ao cidadão nas esferas federal, estadual e municipal.

**1.3** A caracterização dessa oportunidade decorre da constatação de desafios recorrentemente enfrentados por gestores públicos, tais como a necessidade de melhorar a coordenação entre órgãos, integrar bases de dados, ampliar a eficiência operacional ou garantir segurança da informação e conformidade à LGPD. Tais desafios demandam soluções que unam tecnologia, interoperabilidade e inteligência analítica.

**1.4** A solução a ser modelada deverá contemplar **plataforma modular e de arquitetura aberta**, apta a integrar sensores, sistemas de campo e aplicações corporativas, permitindo o monitoramento em tempo real de eventos urbanos, a gestão de incidentes e a orquestração de serviços públicos — tais como **mobilidade e trânsito, segurança pública, defesa civil, iluminação, zeladoria, saneamento, meio ambiente, fiscalização, limpeza urbana e atendimento ao cidadão**.

**1.5** A plataforma deverá possibilitar a **convergência de dados provenientes de múltiplas fontes** (câmeras, sensores ambientais, dispositivos IoT, semáforos inteligentes, rádios, totens, veículos de fiscalização, *apps* de campo e sistemas legados), garantindo interoperabilidade com plataformas municipais, estaduais e federais.

**1.6** O modelo operacional deverá prever **implantação em ambiente de nuvem soberana**, com **escalabilidade horizontal, redundância geográfica e capacidade de operação em contingência (edge/offline)**, assegurando aderência a requisitos técnicos, regulatórios e de segurança da informação, bem como conformidade à Lei Geral de Proteção de Dados (LGPD) e às diretrizes de governança digital do Estado brasileiro.

**1.7** A parceria em estudo deverá ser estruturada nos termos do Art. 28 da Lei nº 13.303/2016 e das diretrizes do Regulamento de Parcerias em Oportunidade de Negócio do SERPRO (RPON), com vistas à composição de arranjos empresariais que integrem competências tecnológicas, especialização de domínio e capacidade operacional. A expectativa é atrair parceiros com experiência comprovada em áreas como Internet das Coisas (IoT), *Edge Computing*, análise de dados, inteligência artificial,

---

infraestrutura de campo e integração com plataformas públicas.

**1.8** Entre os resultados esperados, destacam-se:

- A criação de um ecossistema urbano digital interoperável, capaz de conectar órgãos, sensores e serviços em uma visão integrada;
- A redução de custos e redundâncias operacionais, com base em dados compartilhados e gestão centralizada;
- O aumento da eficiência e da transparência na prestação de serviços públicos;
- O fortalecimento da segurança e da governança da informação, por meio de camadas de proteção, rastreabilidade e conformidade; e
- A ampliação da inteligência analítica aplicada à tomada de decisão, com uso de painéis e indicadores de desempenho.

**1.9** Do ponto de vista estratégico, a iniciativa busca estimular a inovação aberta, atrair empresas com tecnologias complementares e consolidar um modelo de parceria público-estatal sustentável, que una a capacidade de execução da iniciativa privada com a infraestrutura tecnológica, a experiência institucional e a credibilidade do SERPRO como empresa pública de referência em tecnologia e governança digital.

**1.10** Por fim, espera-se construir uma proposta de valor conjunta capaz de posicionar o SERPRO e o(s) parceiro(s) como protagonistas na transformação digital de cidades e operações públicas, em um modelo de negócio escalável, seguro, transparente e aderente às políticas de dados e de governo digital do Estado brasileiro.

## **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 Contexto, Objetivos e Escopo**

**2.2.1** Quais sistemas, módulos ou áreas de atuação sua solução contempla atualmente (por exemplo: COI/CGI/CCO, monitoramento avançado, cercamento eletrônico/LPR, semafórico, IoT, *apps* de campo, portal do cidadão etc.)?

**2.2.2** Como você descreveria o papel da sua empresa nesse ecossistema — por exemplo, fabricante, ISV, integradora, *MSP*/operadora ou uma combinação híbrida?

**2.2.3** Existem dependências de outros parceiros ou fabricantes (como câmeras, controladores, rádios, nuvem)? Como essas relações são geridas e os riscos de *lock-in* são mitigados?

**2.2.4** Qual tem sido a experiência da sua empresa com a Administração Pública, considerando tempo de atuação, esferas (federal, estadual, municipal, distrital) e regiões atendidas?

**2.2.5** Caso aplicável, poderia mencionar contratos públicos recentes ou vigentes que exemplifiquem sua atuação nos últimos três anos?

**2.2.6** Que tipos de escopos ou combinações de módulos seus clientes mais costumam adotar, e como essas entregas são organizadas por fase ou domínio de aplicação?

---

**2.2.7** Quais desafios reais dos clientes públicos sua solução ajuda a resolver (técnicos, operacionais, culturais ou orçamentários) e de que forma o sucesso dessas entregas costuma ser medido?

**2.2.8** Que perfil de contratante tende a obter melhores resultados com sua solução — por exemplo, municípios de determinado porte, infraestrutura pré-existente ou maturidade digital — e quais são os principais pré-requisitos para implantação?

**2.2.9** Já houve questionamentos ou interações com órgãos de controle (TCU, TCE, TCM, CGM, CGU) em seus projetos? Quais foram as lições aprendidas e como sua empresa aprimorou evidências ou controles internos?

**2.2.10** Em sua visão, qual arranjo empresarial é mais adequado para iniciativas desse tipo — empresa única, consórcio, SPE/*joint venture* ou subcontratação especializada — e por quais motivos?

**2.2.11** Em média, quanto tempo leva para implantar sistemas como os de sua solução, e quais fatores costumam representar maiores gargalos ou desafios nesse processo?

**2.2.12** Que fontes de financiamento ou incentivo os contratantes públicos podem acessar para viabilizar projetos dessa natureza (por exemplo, emendas, convênios, fundos setoriais, P&D, BNDES, FUST, PPP ou *performance-based*)?

**2.2.13** Em sua experiência, qual é o prazo contratual mínimo mais adequado (por exemplo, 5, 10 ou 20 anos) para soluções dessa categoria?

**2.2.14** Quais órgãos ou áreas do contratante costumam ser diretamente beneficiados pela implantação da solução (como gestão municipal, segurança, trânsito, defesa civil, zeladoria, TI, planejamento ou turismo)?

### **2.3 Casos de Uso e Operação Urbana**

**2.3.1** Quais casos de uso sua solução contempla hoje, e como eles se relacionam às diferentes necessidades dos municípios (por exemplo, segurança, mobilidade, fiscalização, zeladoria ou defesa civil)?

**2.3.2** Como sua solução trata áreas sensíveis — como escolas, hospitais e zonas residenciais — no que se refere a políticas de acesso, proteção de dados e salvaguardas operacionais?

**2.3.3** De que forma a solução apoia a operação móvel em campo, permitindo que equipes, viaturas e fiscais atuem de forma integrada, mesmo fora do centro de operações?

**2.3.4** Sua solução contempla planos ou estratégias de contingência para situações de emergência, como eventos climáticos, desastres ou grandes aglomerações? Como esses planos são ativados e monitorados na prática?

**2.3.5** Existem procedimentos operacionais ou *playbooks* para diferentes tipos de ocorrência? Como a solução auxilia na execução, atualização e controle desses protocolos?

**2.3.6** A solução favorece a realização de simulações e treinamentos das equipes? De que maneira contribui para o preparo e avaliação de desempenho dos operadores e gestores?

**2.3.7** Como a solução viabiliza a atuação coordenada entre múltiplos órgãos ou secretarias (*multiagência*), preservando a autonomia de cada um e garantindo cooperação operacional quando necessário?

**2.3.8** De que forma são definidos, aplicados e revisados os perfis e permissões de usuários, desde as

---

rotinas operacionais até atividades de auditoria e gestão?

**2.3.9** Há um canal integrado de interação com o cidadão — como *apps*, portais ou centrais — para registro, acompanhamento e avaliação de demandas? Como esse canal se conecta ao centro de operações?

**2.3.10** Quais recursos de monitoramento, painéis e relatórios a solução oferece para apoiar a gestão, a tomada de decisão e a prestação de contas no dia a dia?

## **2.4 Dispositivos, Sensores e Campo**

**2.4.1** Quais tipos de dispositivos sua solução suporta atualmente (por exemplo: câmeras fixas/PTZ, LPR, sensores ambientais, semaforicos, painéis, totens, rádios/LTE, IoT, *edge computing*) e quais limites operacionais costuma adotar por sítio ou área?

**2.4.2** Como os equipamentos utilizados atendem a requisitos de robustez — como graus IP/IK, antivandalismo, faixa térmica, umidade e compatibilidade eletromagnética (EMC) — considerando o uso em ambientes urbanos externos?

**2.4.3** De que forma é feita a gestão do parque em campo, incluindo inventário, telemetria, monitoramento de saúde dos ativos, alertas e histórico de falhas?

**2.4.4** Sua solução prevê mecanismos de contingência no *edge* para quedas de rede (como *buffer*, operação degradada ou sincronização posterior)? Como é garantida a confiabilidade quando o link é restabelecido?

**2.4.5** Quais meios de conectividade são mais utilizados (fibra, rádio licenciado, 4G/5G/LTE privado, Wi-Fi, LoRaWAN) e como é tratada a priorização de tráfego e a qualidade de serviço?

**2.4.6** Como ocorre a comutação entre enlaces e a mitigação de perda de pacotes, *jitter* e latência em cenários críticos?

**2.4.7** Quais práticas ou normas são seguidas para garantir requisitos de energia, proteção elétrica, aterramento e uso de UPS, conforme boas práticas técnicas?

**2.4.8** Existem padrões ou manuais de implantação — como kits, *checklists* e laudos de comissionamento — que facilitem a mobilização, a auditoria e o controle de qualidade?

**2.4.9** Qual é a política adotada para sobressalentes e reposição de campo (níveis mínimos, prazos por região) e como é acompanhado o desempenho operacional dos equipamentos ao longo do tempo?

**2.4.10** Que certificações, homologações ou laudos técnicos se aplicam aos dispositivos utilizados (por exemplo, INMETRO, ANATEL ou equivalentes) e como a empresa comprova conformidade quando necessário?

## **2.5 Software, Integrações e Dados**

**2.5.1** Quais módulos ou componentes de software sua solução oferece (por exemplo: VMS, *analytics*, LPR, CAD/Despacho, GIS, *apps*, portal do cidadão, orquestração) e quais são as principais dependências entre eles?

**2.5.2** Quais padrões ou tecnologias de integração são utilizados (como REST, *webhooks*, gRPC, MQTT/AMQP, OPC-UA)? Como é feito o controle de autenticação e limitação de taxa (*rate limit*)?

**2.5.3** Há um catálogo de APIs ou *SDKs* documentado, com versionamento e ambiente de *sandbox* para terceiros?

---

**2.5.4** Sua arquitetura contempla um barramento de eventos (*pub/sub*) e um modelo de dados documentado, versionado e auditável? Como esse modelo é mantido ao longo do tempo?

**2.5.5** A solução integra-se a sistemas legados municipais ou estaduais (como ouvidoria, protocolo, semafórico, bilhetagem ou iluminação pública)?

**2.5.6** Como a solução lida com dados geoespaciais — como bases cartográficas oficiais, *geofences*, *heatmaps* e camadas temáticas (vias, risco, serviços)?

**2.5.7** Sua solução opera em modo *offline* em algum módulo (*apps*, *edge*)?

**2.5.8** Que tipos de painéis (*dashboards*) e relatórios são oferecidos — em tempo real, históricos ou forenses — e como eles apoiam a análise de desempenho e a tomada de decisão?

**2.5.9** A solução implementa mecanismos de autenticação centralizada (SSO) e controle de acesso baseado em papéis (RBAC/ABAC), com delegação multiagência e registro de acessos?

**2.5.10** Há trilha de auditoria completa (quem, quando, o quê) assinada digitalmente e exportável, em conformidade com a LGPD e normas correlatas?

## **2.6 Arquitetura em Nuvem e Edge**

**2.6.1** Em que tipo de infraestrutura sua solução opera atualmente (*nuvem pública, privada ou híbrida*) e ela é compatível com ambientes de nuvem governamental? Existem restrições ou requisitos específicos?

**2.6.2** Como você descreveria o nível de modernização da arquitetura — ela é *cloud-native*, baseada em microserviços e contêineres, ou segue um modelo mais tradicional (*lift-and-shift*)?

**2.6.3** Há mecanismos de orquestração, como *Kubernetes*, e processos de *CI/CD* estruturados com ambientes segregados, controle de qualidade e auditoria de versões?

**2.6.4** A solução possui recursos de autoescalabilidade e balanceamento de carga para lidar com picos de demanda, como eventos climáticos ou grandes ocorrências urbanas?

**2.6.5** De que forma é garantido o isolamento entre diferentes clientes (*multi-tenant*), incluindo segregação de dados, *backups* e controles de ruído lateral?

**2.6.6** Quais mecanismos de observabilidade são utilizados (métricas, logs, *tracing*) e como esses dados são integrados ao NOC ou SOC da operação?

**2.6.7** Como é feita a comunicação entre o *edge* e a nuvem? Há uso de VPN, TLS mútuo, filas de *retry* ou técnicas de compressão e deduplicação para garantir desempenho e segurança?

**2.6.8** Existem metas definidas de RTO e RPO, planos de *disaster recovery* com redundância geográfica e testes periódicos documentados?

**2.6.9** Como sua empresa comprova a residência dos dados no Brasil e quais mecanismos adota para garantir soberania e conformidade regulatória?

**2.6.10** Quais são os principais SLAs de infraestrutura (disponibilidade, latência, *throughput*) que sua empresa adota, e como são acompanhados e apurados junto aos clientes?

## **2.7 Segurança da Informação e LGPD**

**2.7.1** Quais bases legais da LGPD se aplicam aos fluxos de dados tratados pela sua solução e como

---

essas bases são documentadas ou auditadas (por exemplo, por meio de *RIPD* ou *DPIA*)?

**2.7.2** De que forma a solução incorpora os princípios de *privacy by design* e *privacy by default*, incluindo práticas de minimização, pseudonimização ou mascaramento de dados por finalidade?

**2.7.3** Que mecanismos de criptografia são utilizados em repouso e em trânsito? Como ocorre a gestão e rotação de chaves, uso de *KMS/HSM* e controle de acessos temporários (*Just-In-Time*)?

**2.7.4** Quais controles técnicos e organizacionais são adotados, como autenticação multifator (*MFA*), *hardening*, gestão de vulnerabilidades (*SAST/DAST*), inventário de componentes (*SBOM*) e testes de intrusão independentes?

**2.7.5** A solução se integra a sistemas de segurança como *SIEM* ou SOC, com correlação de eventos e níveis de severidade definidos? Como são tratados os incidentes e tempos de resposta (*SLA*)?

**2.7.6** De que forma é mantida a trilha de auditoria, garantindo integridade, carimbo temporal e cadeia de custódia para fins forenses e de não repúdio?

**2.7.7** Como são definidas e executadas as políticas de retenção e descarte de dados (como vídeo, telemetria, logs), e quais mecanismos asseguram a rastreabilidade e o expurgo auditável?

**2.7.8** Quais procedimentos de *due diligence* são aplicados a terceiros e subprocessadores de dados — como avaliações de segurança, cláusulas contratuais, auditorias ou planos de remediação?

**2.7.9** Existe um plano de resposta a incidentes estruturado, com matriz RACI, prazos legais de comunicação e exercícios práticos de simulação?

**2.7.10** Que certificações, normas ou frameworks de segurança e privacidade sua empresa adota (como ISO 27001, ISO 27701, NIST CSF) e qual foi a última auditoria ou avaliação de conformidade realizada?

## **2.8 Analytics e Inteligência Artificial**

**2.8.1** Quais módulos ou recursos de *analytics* e Inteligência Artificial sua solução oferece (como detecção de incidentes, LPR, previsão de eventos, fusão multissensorial) e quais casos de uso exemplificam sua aplicação prática?

**2.8.2** Os modelos utilizados são treináveis ou adaptáveis ao contexto local (como clima, geografia, padrões urbanos)? Quais tipos de dados alimentam esses processos de aprendizado?

**2.8.3** Sua empresa mantém um fluxo estruturado de *MLOps*, com práticas de treino, validação, versionamento, *deployment* e monitoramento de *drift* de modelos?

**2.8.4** Existem mecanismos de explicabilidade — como *SHAP*, *LIME* ou outros — que permitam compreender e auditar decisões automatizadas?

**2.8.5** A solução oferece capacidade de inferência no *edge*, com operação *offline* e sincronização posterior segura, mantendo controle sobre versões e modelos?

**2.8.6** Quais métricas de desempenho são utilizadas para avaliar os modelos (acurácia, precisão, *recall*, *FPR/FNR*) e com que periodicidade são revisadas?

**2.8.7** Como sua empresa trata e mitiga possíveis vieses nos dados, nos modelos ou na operação? Há práticas de reporte e transparência sobre esses resultados por grupos populacionais?

**2.8.8** A solução permite orquestrar automações baseadas em regras (*BPMN*) e eventos de IA — como despacho automático ou controle adaptativo de semáforos?

---

**2.8.9** Quais tipos de *APIs* são expostas para exportar *features* ou *insights*, e para permitir auditoria de modelos, decisões e parâmetros utilizados?

**2.8.10** Há um *roadmap* de evolução da IA para os próximos 12 a 24 meses, indicando novas funcionalidades, critérios de aceitação, impactos esperados em custo, infraestrutura e segurança?

## **2.9 Mobilidade, Trânsito e Fluxos**

**2.9.1** Sua solução integra controladores semafóricos, planos e fases de operação?

**2.9.2** De que forma coleta e analisa dados de volume, velocidade e ocupação das vias, e como essas informações são utilizadas no planejamento viário ou disponibilizadas via *APIs* e relatórios?

**2.9.3** Há integração com radares, sistemas de fiscalização e registros de eventos de tráfego? C

**2.9.4** No módulo de LPR (*License Plate Recognition*), quais atributos são extraídos (placa, marca, cor, modelo), quais níveis de acurácia são observados e como são aplicadas as políticas de retenção e anonimização?

**2.9.5** A solução gera rotas de emergência e aplica prioridade semaforica dinâmica? Quais critérios e indicadores de efetividade são utilizados nesses cenários?

**2.9.6** Existe integração com painéis informativos ou sistemas de sinalização dinâmica? Como são definidas as regras de publicação, os horários e as contingências operacionais?

**2.9.7** Sua solução realiza análises de *hotspots* de acidentes ou incidentes? Como essas informações são traduzidas em recomendações para engenharia, fiscalização ou educação no trânsito?

**2.9.8** Há integração com sistemas de transporte público — como GPS da frota, intervalos de operação (*headway*) e indicadores de lotação — com alertas de desvios em tempo real?

**2.9.9** De que forma a solução apoia a gestão de interdições e eventos urbanos, incluindo geração automática de desvios e comunicação ao cidadão?

**2.9.10** A solução disponibiliza dados abertos sobre mobilidade e trânsito? Quais formatos, padrões e licenças adota para garantir anonimização e reuso responsável das informações?

## **2.10 Defesa Civil, Clima e Risco**

**2.10.1** Sua solução integra sensores hidrológicos, pluviômetros ou dados meteorológicos? Quais fontes utiliza e como são definidos os gatilhos automáticos de alerta?

**2.10.2** São mapeadas as áreas de risco, como alagamentos ou deslizamentos, e de que forma a solução representa níveis de criticidade e históricos desses eventos?

**2.10.3** Há funcionalidades para disparo de sirenes, envio de mensagens públicas ou despacho de equipes em campo? Como são monitorados o rastreamento e o tempo de resposta (*SLA*)?

**2.10.4** Sua solução contempla simulações e exercícios de desastre? Como são gerados os planos de contingência e avaliadas as lições aprendidas após os testes?

**2.10.5** É possível integrar rotas de evacuação, abrigos e pontos de apoio, acompanhando a ocupação desses locais em tempo real?

**2.10.6** Como são registrados os danos, vistorias e laudos de campo — incluindo fotos, georreferenciamento e carimbo de tempo?



---

**2.10.7** Há consolidação de indicadores pós-evento (como tempo de resposta, extensão de danos e ações executadas) para fins de prestação de contas e auditoria?

**2.10.8** Sua solução opera com redundância de energia e comunicação em crises, como geradores, enlaces alternativos ou conectividade satelital?

**2.10.9** De que maneira são enviadas mensagens à população — por SMS, *push notifications*, WhatsApp ou web — e como ocorre o direcionamento por área ou perfil?

**2.10.10** A solução se integra a órgãos estaduais ou federais (como Defesa Civil, meteorologia ou alertas nacionais)? Quais padrões ou protocolos adota nessa interoperabilidade?

## **2.11 Acessibilidade, Inclusão e Cidadão**

**2.11.1** As interfaces da sua solução seguem diretrizes de acessibilidade como WCAG/W3C e a norma ABNT NBR 9050?

**2.11.2** Que recursos assistivos estão disponíveis — como contraste, leitor de tela, atalhos de navegação, tradução em LIBRAS ou legendas automáticas — e como são testados com usuários reais?

**2.11.3** Os *apps* móveis contemplam recursos de acessibilidade, como ajuste de tamanho de fonte, navegação por voz ou retorno tátil (*feedback háptico*)? Há exemplos práticos de uso?

**2.11.4** Como a solução trata áreas sensíveis e grupos vulneráveis, garantindo anonimização, perfis diferenciados e políticas de proteção específicas?

**2.11.5** De que forma é feito o registro e a gestão do consentimento de usuários, quando aplicável, assegurando rastreabilidade e trilha de auditoria das manifestações de ciência?

**2.11.6** Há materiais de apoio acessíveis — como vídeos com audiodescrição, linguagem simples, múltiplos formatos ou idiomas? Como são produzidos e atualizados?

**2.11.7** Os fluxos de atendimento consideram prioridades legais (idosos, pessoas com deficiência, gestantes, emergências)? Quais indicadores medem o atendimento a esses públicos?

**2.11.8** Em caso de falhas nos módulos digitais, há canais alternativos de atendimento — como suporte humano, telefone ou protocolo presencial — com tempos de resposta definidos (*SLA*)?

**2.11.9** Sua empresa mede a satisfação do usuário final (como *NPS* ou *CSAT*)? Como são tratadas as barreiras identificadas e implementadas melhorias contínuas?

**2.11.10** Há políticas de transparência ativa e publicação de dados abertos relacionados à cidadania e inclusão?

## **2.12 Operação, Suporte e ITSM**

**2.12.1** Como é estruturado o suporte técnico da sua solução — ele opera em regime 24x7 (níveis N1 a N3)? Quais canais, idiomas e tempos de resposta costumam ser oferecidos?

**2.12.2** Quais indicadores de desempenho (como *MTTR*, *MTBF* e disponibilidade efetiva) são acompanhados, e quais metas costumam ser praticadas por nível de criticidade?

**2.12.3** Que ferramentas de *ITSM* são utilizadas para gestão de incidentes, problemas, mudanças e ativos (*CMDB*)? Há integrações via *APIs* ou *webhooks* com outros sistemas?

**2.12.4** Sua empresa adota monitoração proativa (*health checks*, *SLIs/SLOs*), alertas automáticos e



---

mecanismos de escalonamento? Como essas práticas se conectam à operação em campo?

**2.12.5** Como é conduzida a manutenção preventiva e preditiva em campo? Qual a periodicidade, os principais indicadores de desempenho e as formas de comprovação utilizadas?

**2.12.6** De que maneira a gestão de mudanças é estruturada — há comitês (CAB), janelas planejadas, mecanismos de *rollback* e trilhas de auditoria por ambiente?

**2.12.7** Sua empresa mantém planos de continuidade de negócios (BCP), contingência e *disaster recovery*? Com que frequência são testados e revisados os tempos de RTO/RPO?

**2.12.8** Quais treinamentos são oferecidos para operadores e gestores? Há carga horária definida, materiais de apoio e programas de reciclagem periódica?

**2.12.9** Existem *runbooks* ou *playbooks* por tipo de incidente ou ocorrência? Como são definidos os gatilhos e critérios de encerramento de cada tipo de evento?

**2.12.10** Como a empresa mede a satisfação com o suporte (como NPS ou CSAT) e conduz o plano de melhorias contínuas a partir do feedback dos usuários?

## **2.13 Comercial, Financeiro e Contratual**

**2.13.1** Quais modelos de contratação sua empresa costuma oferecer (como compra, *leasing*, *SaaS*, *BPO*/gestão ou formatos híbridos)? Em quais situações cada modelo é mais adequado?

**2.13.2** Como é estruturada a precificação dos serviços — por uso, dispositivo, evento, volume de dados ou número de usuários?

**2.13.3** Existem taxas de mobilização, implantação ou custos recorrentes (suporte, nuvem, manutenção de campo)?

**2.13.4** Que tipos de SLAs financeiros são aplicados — como faixas de abatimento por indisponibilidade ou descumprimento de indicadores? Há limites e exceções previstos?

**2.13.5** Os contratos permitem elasticidade de consumo (crescimento ou redução) com reprecificação automática por faixas de volume? Como essa flexibilidade é administrada?

**2.13.6** Sua empresa adota modelos de remuneração baseados em performance — como *gain share*, *pay-per-use* ou *pay-per-outcome*?

**2.13.7** Como são definidos os reajustes contratuais (IPCA, IGP-M, câmbio) e quais práticas são aplicadas para mitigar riscos de variação cambial ou de custos importados?

**2.13.8** Quais políticas garantem a portabilidade e reversibilidade ao término do contrato, incluindo exportação de dados, abertura de *APIs*, documentação técnica e transferência de conhecimento?

**2.13.9** Há políticas de descontos ou condições diferenciadas para consórcios intermunicipais, contratos multisecretariais ou expansões dentro da mesma administração pública?

## **2.14 Regulação e Normas**

**2.14.1** Quais normas técnicas ou regulatórias se aplicam à sua solução (como CFTV/LPR, rádios/ANATEL, semafórico/CONTRAN/ABNT, IoT)? Como sua empresa comprova aderência ou conformidade a essas exigências?

**2.14.2** Existem requisitos ou legislações municipais e estaduais relacionados ao videomonitoramento,

---

sinalização ou uso de imagens em áreas públicas?

**2.14.3** Para componentes de mobilidade e trânsito, como são atendidas as exigências do Órgão Nacional de Trânsito e normas ABNT (controladores, sincronismo, registro de infrações, dados de tráfego)?

**2.14.4** Que tipos de anuências, licenças ou autorizações são necessárias para implantação (como uso de postes, prédios públicos, patrimônio histórico ou meio ambiente)? Quais são os prazos e práticas adotadas para obtê-las?

**2.14.5** Existem restrições operacionais em áreas sensíveis (como escolas, hospitais ou residências)? Quais políticas de zonas de privacidade ou delimitação são aplicadas nesses casos?

**2.14.6** Sua solução já participou de pilotos, *sandboxes* regulatórios ou certificações setoriais em municípios, estados ou órgãos federais? Quais resultados ou aprendizados decorreram dessas experiências?

## **2.15 Sustentabilidade (ESG)**

**2.15.1** Sua empresa mantém inventário de emissões de gases de efeito estufa (*GEE*)? Existem metas de redução e práticas de uso de energia renovável (como certificados *I-REC*)?

**2.15.2** Quais medidas de eficiência energética são adotadas — como controle de *PUE/DCiE* em data centers, modos de economia em equipamentos *edge*, consolidação ou virtualização de recursos?

**2.15.3** Há políticas de logística reversa para descarte de equipamentos, *e-lixo* e embalagens? Como são tratados o reuso, o reparo e a certificação ambiental dos materiais?

**2.15.4** Quais políticas internas abordam diversidade, equidade e inclusão (*DEI*), direitos humanos, saúde e segurança ocupacional (NRs) e canais de denúncia? Existem indicadores de acompanhamento público?

**2.15.5** Sua empresa promove programas de capacitação técnica ou socioambiental para clientes, parceiros ou colaboradores? Qual a carga horária média e como é feita a comprovação?

**2.15.6** Há processos de *due diligence* socioambiental aplicados a fornecedores e subcontratados, incluindo cláusulas contratuais e planos de conformidade em *ESG*?

**2.15.7** Quais indicadores de *ESG* são acompanhados em contrato (por exemplo, disponibilidade verde, descarte adequado, acidentes, diversidade)? Com que frequência são reportados?

**2.15.8** Sua empresa publica relatórios de sustentabilidade (como GRI, SASB ou TCFD) ou auditorias independentes (*ISAE*, *SOC*)? Poderia mencionar o escopo e a edição mais recente?

**2.15.9** Existem ações voltadas à redução de deslocamentos e otimização logística (como planejamento de rotas, uso de frota elétrica ou híbrida)? Que resultados já foram obtidos?

**2.15.10** Há planos de melhoria contínua em *ESG*, com metas, responsáveis, prazos e mecanismos de acompanhamento? Como são registradas e divulgadas as lições aprendidas?

## **2.16 Implantação, POC e Referências**

**2.16.1** Qual metodologia de implantação ou *rollout* sua empresa adota (por fases, ondas, módulos)?

**2.16.2** Quais são os tempos médios de implantação por tipo de sítio (câmera fixa/PTZ/LPR, sensor, controlador semafórico, totem, rádio/backhaul, *edge box*)?

---

**2.16.3** Qual a capacidade média de instalação semanal ou mensal (em pontos por dia ou *squads* simultâneos) e quais fatores costumam limitar o ritmo de implantação?

**2.16.4** Como é realizado o comissionamento dos equipamentos e sistemas — há registros fotográficos, georreferenciamento, laudos técnicos e critérios de aceitação provisória e definitiva?

**2.16.5** Quais estratégias são utilizadas para migração de legados, garantindo continuidade do serviço — como operação paralela, *cut-over* gradual ou implantação em ondas?

**2.16.6** Sua empresa já executou projetos-piloto ou *POCs*? Quais foram os objetivos, critérios de sucesso e principais resultados obtidos?

**2.16.7** Como são estruturados os treinamentos para diferentes perfis (operadores, supervisores, gestores, equipe de TI)? Qual a carga horária e formato (presencial, on-line, híbrido)?

**2.16.8** Há um período de estabilização após o *go-live*? Como é organizada a equipe dedicada e o processo de *handover* para a operação titular?

**2.16.9** Quais riscos de implantação são mais recorrentes (logística, importação, obra civil, energia, interferências) e que estratégias de mitigação são adotadas?

**2.16.10** Poderia citar referências de projetos no Brasil, incluindo órgão ou município, ano, módulos implantados, níveis de SLA alcançados e, se possível, contatos autorizados para verificação?

## **2.17 Contratos com Entes Públicos**

**2.17.1** Possui contratos públicos celebrados nos últimos três anos?

**2.17.2** Quais modalidades de contratação foram utilizadas (como concorrência, pregão, *SRP/ata*, dispensa, PPP, concessão ou convênio) e que aprendizados surgiram dessas experiências?

**2.17.3** Houve aditivos de prazo, valor ou escopo em contratos anteriores? Quais foram as causas mais comuns, os impactos e as medidas adotadas para evitar recorrências?

**2.17.4** Sua empresa possui cartas ou atestados de capacidade técnica? Poderia comentar os principais escopos e volumes atestados nesses documentos?

**2.17.5** Já ocorreram glosas ou penalidades contratuais? Quais foram os motivos e como a empresa tratou essas situações para evitar reincidências?

**2.17.6** Qual é o ticket médio dos contratos por porte de município (pequeno, médio, grande)? Quais fatores mais influenciam as variações de custo e escopo?

**2.17.7** Em casos de adesão a atas de registro de preços (*SRP*), qual tem sido a taxa média de adesão, o perfil das regiões participantes e as variações sazonais observadas?

## **2.18 Valores de Mercado, TCO e Precificação**

**2.18.1** Quais faixas de preço são praticadas, em média, por tipo de dispositivo (como câmera fixa/PTZ, LPR, totem, rádio licenciado ou controlador semafórico)?

**2.18.2** Como é estruturado o custo mensal (*OPEX*) dos módulos de software — por canal, volume de dados (*GB*), número de usuários ou dispositivos — e como ocorre a medição e auditoria desse uso?

**2.18.3** Qual seria o *Total Cost of Ownership (TCO)* estimado em cinco anos para cenários de diferentes portes (ex.: 50, 300 e 1.000 pontos)? Quais premissas e variáveis são mais sensíveis nesse cálculo?

---

**2.18.4** Existem degraus de preço ou políticas de desconto por volume, consórcio ou região? Quais critérios orientam essas variações?

**2.18.5** Há taxas de mobilização, implantação ou comissionamento? Como elas são calculadas e amortizadas ao longo do contrato?

**2.18.6** Quais custos médios de nuvem são considerados (R\$/mês por TB ou Gbps) e que estratégias de otimização — como *tiering*, compressão ou retenção — são aplicadas para reduzir despesas?

**2.18.7** Quais são os custos típicos de conectividade por ponto/mês (4G, 5G, rádio licenciado, fibra) e como variam conforme região ou operadora?

**2.18.8** Como é definido o custo de suporte e *ITSM* por dispositivo ou usuário? Que níveis de serviço (N1–N3) estão associados a esses valores?

**2.18.9** Quais são os custos médios de manutenção de campo (preventiva e corretiva) por ponto/ano, e como são estruturados os prazos e SLAs de atendimento?

**2.18.10** Que índices de reajuste (IPCA, IGP-M) e políticas cambiais são aplicados para itens importados? Há mecanismos contratuais de proteção contra variação de preços?

**2.18.11** Como sua empresa trata SLAs financeiros — há faixas de abatimento por indisponibilidade ou descumprimento de indicadores? Quais limites e exceções são previstos?

**2.18.12** Modelos *pay-per-use* (por evento, alerta ou processamento) são utilizados? Como é feita a medição e validação independente desses resultados?

**2.18.13** Sua empresa já operou contratos temporários voltados a eventos específicos (*monta/opera/desmonta*)? Há tabelas sazonais de preço ou pacotes curtos de operação?

**2.18.14** Quais riscos mais impactam a estrutura de custos (como câmbio, energia, logística, armazenamento)? Que estratégias de mitigação são aplicadas?

**2.18.15** Como costuma ser distribuído o custo total entre os módulos — por exemplo, VMS, LPR, CAD, IoT, conectividade, nuvem e suporte?

## **2.19 Arranjos de Entrega (Integrador, Fabricante, Consórcio e Outros Modelos)**

**2.19.1** Para o seu portfólio atual, quais modelos de entrega têm se mostrado mais eficazes — atuação como integrador, fabricante *full-stack*, consórcio, *joint venture*, SPE, parceria operacional, *white-label* ou modelo de operador gerenciado (*managed service provider*)?

**2.19.2** Como sua empresa gerencia os riscos de interface entre diferentes componentes e fornecedores (hardware, software, campo, conectividade e nuvem)? Há uma matriz de responsabilidades (RACI) ou prática equivalente formalizada?

**2.19.3** Existem SLAs internos ou acordos de nível de serviço entre os membros do arranjo? Como são medidos o desempenho conjunto, o tempo de resposta (*MTTR multi-vendor*) e a qualidade integrada da entrega?

**2.19.4** Sua empresa possui cobertura nacional por meio de rede própria ou de parceiros regionais? Quais regiões estão cobertas e como é comprovada a capacidade de execução técnica e logística?

**2.19.5** Existem cláusulas contratuais entre os participantes ou com o cliente que assegurem interoperabilidade, evitem *lock-in* e garantam portabilidade, APIs abertas e transferência de *know-how*?

---

**2.19.6** Em sua avaliação, em quais contextos o modelo com fabricante-líder, integrador-líder, operador gerenciado ou parceiro *white-label* tende a ser mais vantajoso? Quais critérios objetivos orientam essa decisão?

**2.20 Implantação, Portfólio, Tendências e Governança**

**2.20.1** Quais estratégias sua empresa adota para reduzir prazos de implantação e acelerar o *time-to-value* em projetos complexos? Há boas práticas específicas para entes públicos?

**2.20.2** Como é garantida a qualidade da entrega em implantações simultâneas em múltiplas cidades ou órgãos, considerando logística, supervisão e aceites técnicos?

**2.20.3** Como sua empresa enxerga a divisão ideal de responsabilidades em um modelo de parceria com o Serpro — considerando papéis técnicos, operacionais e comerciais?

**2.20.4** Quais indicadores de desempenho ou resultados poderiam compor um modelo de *revenue share* ou contrato orientado a performance, assegurando equilíbrio e sustentabilidade para ambas as partes?

**2.20.5** Que práticas de transparência, auditoria e prestação de contas sua empresa recomenda para parcerias público-estatais, especialmente em contratos de longo prazo ou com uso intensivo de dados?

**2.20.6** Como sua empresa planeja evoluir tecnologicamente seu portfólio (próximos 12–24 meses)?