EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A

EDITAL DE CHAMAMENTO PÚBLICO PRODAM-SP S/A Nº [XXX/2026]
PROCESSO SEI N° XXXX.XXXX/XXXXXXX-X

OBJETO: Chamamento Público para seleção de pessoa jurídica de direito privado (empresas) que, em parceria com a PRODAM-SP S/A, possa explorar a oportunidade de negócio especificada no ANEXO I.

A EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A, sociedade de economia mista, com sede na Rua Libero Badaró, 425, Centro, São Paulo - SP, inscrita no CNPJ/MF sob o nº 43.076.702/0001-61, considerando os princípios da isonomia, da impessoalidade, da publicidade, da eficiência e do julgamento objetivo, torna público o presente chamamento público para selecionar pessoa jurídica de direito privado, que iniciará a partir da publicação deste Edital e seus anexos.

O processo será regido pelo art. 28, § 3º, inc. II, e § 4º, da Lei nº 13.303/2016, pelo Regulamento de Parceria em Oportunidade de Negócios e, no que couber, pelo Regulamento Interno de Licitações e Contratos da PRODAM-SP e demais condições fixadas neste Edital e seus Anexos.

EDITAL DE CHAMAMENTO PÚBLICO PARA SELEÇÃO DE PARCEIRO PRIVADO	
Edital Nº	[XXX/2026]
Objeto	
Entidade	EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A
Fundamentação Legal Principal	Art. 28, § 3º, inc. II, e § 4º, da Lei nº 13.303/2016; Regulamento de Parcerias em Oportunidade de Negócios; Regulamento Interno de Licitações e Contratos da PRODAM-SP.
Endereço Eletrônico (Dúvidas/Propostas)	[parceria-objeto@prodam.sp.gov.br]
Sítio de Publicação	[https://portal.prodam.sp.gov.br/licitacoes]

Anexos	**I:** Plano de Negócio Preliminar da Oportunidade **II:** Roteiro e Critérios de Avaliação da Prova de Conceito (POC) **III:** Requisitos da Proposta **IV:** Planilha de Requisitos Técnicos da Solução e Critérios de Pontuação **V:** Planilha de Capacidade Técnica do Parceiro **VI**: Minuta-padrão de Contrato Associativo (Anexos A, B, C, D e E) **VII:** Declaração de Transação com Parte Relacionada **VIII**: Declaração de Ausência de Impedimento para Contratar com a PRODAM-SP
Prazos	(Definidos na Seção II - Do Cronograma das Fases)

SEÇÃO I - DO OBJETO E DA FUNDAMENTAÇÃO LEGAL

1.1. O objeto do presente Edital e seus anexos, na forma do art. 28, § 3º, inc. II, da Lei nº 13.303/2016, é a realização de chamamento público destinado a selecionar pessoa jurídica de direito privado, adiante chamada(s) de INTERESSADA(S), para, em parceria com a PRODAM-SP, explorar oportunidade de negócio específica e definida, conforme **ANEXO I (Plano de Negócio Preliminar da Oportunidade de Negócio)**.

1.2. A atuação em parceria se dará para a construção de produto ou serviço (solução) a ser comercializado pelas PARCEIRAS, em conformidade com as suas respectivas políticas, interesses, procedimentos e processos inerentes de cada instituição.

1.3. A parceria é a relação jurídica constituída por um Contrato de Parceria em Oportunidade de Negócio, que é contrato de espécie associativa.

1.3.1. Em razão da natureza associativa do contrato, enfatiza-se que o presente Edital não se refere a uma relação de fornecimento e consumo, não garante resultados e não visa constituir sociedade empresarial entre os parceiros, cujo objeto se caracteriza, na linguagem corrente empresarial, como *joint-venture* contratual, mas nunca societária.

SEÇÃO II - DO CRONOGRAMA DAS FASES

2.1. O presente Chamamento Público será conduzido em duas fases distintas, sucessivas e interdependentes (Habilitação e Julgamento), conforme o cronograma abaixo.

A estruturação em duas fases visa garantir, primeiramente, a qualificação técnica, jurídica e fiscal mínima de todos os proponentes, bem como a análise do modelo de negócios apresentado (Fase 1) e, subsequentemente, selecionar a proposta de parceria mais vantajosa para a PRODAM-SP com base na Prova de Conceito realizada (Fase 2).

Tabela 1: Cronograma do Chamamento Público

Fase	**Etapa**	**Data/Prazo**
-	Publicação do Edital	
-	Pedidos de Esclarecimento e Impugnação	Até 5 (cinco) dias úteis antes do término da Fase 1
FASE 1 **(Habilitação e Classificação)**	**Prazo final para Envio da Documentação (Jurídica, Fiscal e Regularidade) e Apresentação da Proposta de Modelo de Negócio e Qualificação da Proposta (Anexos III, IV e V)**	**30 (trinta) dias corridos após a Publicação do Edital**
FASE 1 **(Habilitação e Classificação)**	Publicação do Resultado Provisório da Habilitação e Classificação	
-	Prazo Recursal (sobre a Fase 1)	5 (cinco) dias úteis
FASE 2 (Julgamento)	Convocação para a Prova de Conceito (POC)	A ser agendada pela Comissão
FASE 2 (Julgamento)	Realização da Prova de Conceito (POC) (Anexo II)	[Período a ser definido pela Comissão, que será informado

		no momento da Convocação
FASE 2 (Julgamento)	Publicação do Resultado Final do Chamamento	
	Prazo Recursal (sobre a Fase 2)	5 (cinco) dias úteis
-	Convocação da(s) Vencedora(s) (Avaliação de Integridade)	

2.2. Todos os horários estabelecidos neste edital observarão o horário de Brasília - DF.

2.3. Na contagem dos prazos estabelecidos neste edital, o dia do início é excluído e o dia do vencimento é incluído. Só se iniciam e vencem os prazos em dias de expediente na PRODAM-SP.

SEÇÃO III - DA IMPUGNAÇÃO E DOS PEDIDOS DE ESCLARECIMENTO

3.1. O pedido de esclarecimento e/ou de impugnação deverá observar a forma escrita e indicar a qualificação da INTERESSADA (razão social, CNPJ, nome e CPF de seu representante), devendo conter os endereços físico e eletrônico, e o telefone.

3.2. Eventual Pedido de Esclarecimento em relação a dúvidas na interpretação deste edital e seus anexos deverá ser encaminhado ao endereço eletrônico informado no preâmbulo, em até 05 (cinco) dias úteis antes do prazo final para envio da documentação da Fase 1 (item 2.1).

3.3. Qualquer pessoa poderá impugnar o edital em até 05 (cinco) dias úteis antes do prazo final para envio da documentação da Fase 1, devendo encaminhar a impugnação ao endereço eletrônico informado no preâmbulo, contendo a indicação específica e objetiva de cada item que se pretende impugnar, com a respectiva fundamentação. A impugnação não possui efeito suspensivo.

3.4. Caberá à PRODAM-SP decidir sobre a impugnação e/ou responder sobre o pedido de esclarecimento no prazo de 03 (três) dias úteis, publicando sua resposta no sítio informado no preâmbulo.

SEÇÃO IV - DA ESTRUTURA DO PROCESSO SELETIVO

4.1. O presente chamamento público é estruturado em duas fases distintas e sucessivas, sendo a primeira de Habilitação e Classificação e a segunda de Julgamento.

4.2. FASE 1: HABILITAÇÃO e CLASSIFICAÇÃO:

4.2.1. Esta fase visa aferir a capacidade jurídica, a regularidade fiscal e a aptidão técnica mínima das INTERESSADAS para a execução do objeto da parceria, bem como a análise do modelo de negócios apresentado.

4.2.2. A Fase 1 consiste em duas etapas sucessivas:

a) Análise Documental: Verificação da integralidade e conformidade dos documentos de Habilitação Jurídica, Fiscal e de Regularidade (item 5.2).

b) Análise do modelo de negócios apresentado: A pontuação e a classificação serão baseadas exclusivamente nos critérios definidos nos ANEXO III, IV e V.

4.2.3. O resultado de cada INTERESSADA em relação ao item 4.2.2.a) será binário, sendo declarada "Habilitada" ou "Inabilitada".

4.2.4. O resultado de cada INTERESSADA em relação ao item 4.2.2.b) visa avaliar e classificar, por meio de pontuação, a proposta de parceria e o modelo de negócios apresentado, selecionando a(s) proposta(s) tecnicamente mais vantajosa(s) para a PRODAM-SP.

4.2.5. Ao término da Fase 1, será divulgado o Resultado Provisório da Habilitação e Classificação, nos termos do cronograma estabelecido na Seção II deste Edital.

4.3. FASE 2: JULGAMENTO:

4.3.1. Esta Fase destina-se exclusivamente às INTERESSADAS habilitadas e classificadas até o 3º (terceiro) lugar na Fase 1, que serão convocadas para a realização da Prova de Conceito – POC

4.3.2. O Julgamento da Fase 2 consistirá na Análise Prática (Prova de Conceito - POC): Realização de testes práticos, conforme ANEXO II, para comprovar o atendimento aos requisitos funcionais mínimos da solução proposta.

4.3.3. Durante a realização da Prova de Conceito – POC, caso seja constatada característica incompatível com a documentação apresentada na fase anterior, a nota provisoriamente atribuída poderá ser revista, mediante a devida justificativa.

4.3.4. Após o Julgamento, caso as 3 (três) INTERESSADAS sejam habilitadas na prova de conceito, será constituído Cadastro de Reserva.

SEÇÃO V - DA HABILITAÇÃO TÉCNICA E JURÍDICA

5.1. Do Prazo e Envio da Documentação

5.1.1. A(s) INTERESSADA(S) deverá(ão) encaminhar, até o prazo final estabelecido na Seção II (Cronograma), a totalidade dos documentos de Habilitação (subseções 5.2 e 5.3) ao endereço eletrônico informado no preâmbulo.

5.1.2. A não apresentação de qualquer documento exigido nesta fase, ou sua apresentação em desacordo com este edital e seus anexos, implicará na inabilitação sumária da(s) INTERESSADA(S).

5.2. Da Documentação de Habilitação Jurídica, Fiscal e de Regularidade

5.2.1. A(s) INTERESSADA(S) deverá(ão) apresentar os seguintes documentos:

a) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.

b) Declaração conforme modelos do ANEXO VII e do ANEXO VIII, de que não está enquadrada em nenhuma das vedações, inclusive aquelas previstas no art. 38 da Lei nº 13.303/2016.

c) Certidão Negativa de Falência ou Recuperação Judicial expedida pelo Distribuidor da sede da pessoa jurídica, em data não superior a 90 (noventa) dias da data de apresentação da proposta, se outro prazo não constar do documento.

c.1) Caso a INTERESSADA seja cooperativa ou sociedade não empresária, a certidão mencionada no subitem 5.2.1.c deverá ser substituída por Certidão Negativa de Ações de Insolvência Civil.

d) Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada sua substituição por Balancetes ou Balanços Provisórios, exigindo-se, nos casos de sociedade comercial e civil, o Termo de Abertura e Encerramento.

d.1) No caso de empresa constituída há menos de 1 (um) ano, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

d.2) Caso o documento não seja cópia do livro diário da empresa, deverá ser informado à parte, a numeração do livro e das páginas, onde tenham sido lançados, ressalvado o disposto no § 2º do artigo 1.179 do Código Civil.

d.3) O não cumprimento do subitem 5.2.1.d.2, não constitui motivo para inabilitação da INTERESSADA, ficando reservado à PRODAM-SP o direito de exigir o livro diário da empresa, para quaisquer verificações.

d.4) No caso de sociedade anônima deverá ser apresentada a cópia da publicação do Balanço em jornal de grande circulação ou Diário Oficial, exceto os casos previstos na Lei Federal nº 13.818/2019.

d.5) As empresas obrigadas a escrituração por meio do SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL-SPED, conforme previsto no § 3º do art. 11 da Lei Federal nº 8.218, de 29 de agosto de 1991 e art. 16 da Lei Federal nº 9.779, de 19 de janeiro de 1999, deverão apresentar os seguintes impressos do arquivo SPED Contábil:

- Termo de Abertura e Encerramento
- Balanço Patrimonial
- Demonstrativo de Resultado do Exercício (DRE)
- Recibo de Entrega do Livro Digital

e) Apresentar no mínimo 1 (um) indicador dentre os 3 (três) abaixo listados, com resultado igual ou superior a 1 (um), cada:

$$\text{e.1. Liquidez Corrente} = \frac{\textit{Ativo Circulante}}{\textit{Passivo Circulante}} \geq 1$$

$$\text{e.2. Liquidez Geral} = \frac{\textit{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\textit{Passivo Circulante} + \textit{Exigível a Longo Prazo}} \geq 1$$

$$\text{e.3 Solvência Geral} = \frac{\textit{Ativo Total}}{\textit{Passivo Circulante} + \textit{Exigível a Longo Prazo}} \geq 1$$

f) Formulário de Declaração de Transação com Parte Relacionada e Nepotismo, conforme modelos dos ANEXOS VII e VIII.

5.2.2. A PRODAM-SP verificará a regularidade da INTERESSADA por meio de consulta aos seguintes cadastros:

a) Cadastro Nacional de Empresas Inidôneas ou Suspensas (CEIS) e Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa (CNCIAI).

b) Certidão de regularidade junto ao Fundo de Garantia por Tempo de Serviço (FGTS).

c) Certidão Negativa de Débitos (CND) relativos a tributos federais, estaduais e municipais (do domicílio ou sede da INTERESSADA) e à Dívida Ativa da União, expedida pela Receita Federal do Brasil (RFB) e Secretarias de Fazenda competentes.

5.2.3. Poderão ser admitidas para este chamamento público INTERESSADAS reunidas em Consórcio dada a complexidade da solução proposta.

5.2.4. Para fins de análise de requisitos, a verificação pela PRODAM em sítios eletrônicos oficiais, de órgão e entidades emissoras de certidões, constitui meio legal de prova.

5.2.5. Da participação de INTERESSADAS estrangeiras:

5.2.5.1. As INTERESSADAS estrangeiras poderão participar por meio de filial, sucursal, agência ou estabelecimento no Brasil, cumprindo as condições exigidas nos itens anteriores.

5.2.5.2. As INTERESSADAS estrangeiras que não tenham filial, sucursal, agência ou estabelecimento no Brasil, podem participar desde que comprovem os requisitos segundo a tabela:

Requisito Interessadas Estrangeiras	Forma de demonstração
5.2.5.2.1 Habilitação jurídica e fiscal equivalentes, em seu país, aos exigidos nos itens anteriores desta Seção	Meios usuais no país de origem, desde que equivalentes aos meios brasileiros,
5.2.5.2.2 Capacidade jurídica do representante que, em nome da INTERESSADA, firmará a Proposta;	Apresentação de procuração ou outro instrumento em que conste a transferência de poderes.
5.2.5.2.3 Autorização de funcionamento expedida pelo Governo Federal	Apresentação do decreto de autorização.

5.3. Da Apresentação da Proposta de Modelo de Negócio

5.3.1. As INTERESSADAS terão o prazo definido na Seção II (Cronograma) para elaborar e encaminhar suas Propostas de Modelo de Negócios ao endereço eletrônico do certame.

5.3.2. A Proposta de Modelo de Negócio deverá ser elaborada em observância ao Plano de Negócio Preliminar da Oportunidade (ANEXO I) e em consonância o conteúdo mínimo exigido nos **ANEXOS III, IV e V.**

5.3.3. A omissão de qualquer elemento solicitado ou a apresentação de propostas com vícios, poderão ter a atribuição de pontos prejudicada, nos termos do Anexos. Se a informação faltante for essencial ao modelo de negócio, a proposta poderá ser desclassificada.

5.3.3.1. Propostas que não estejam redigidas em língua portuguesa ou que não apresentem valores expressos em reais (R$) implicarão na desclassificação da proposta.

5.4. Do Julgamento da Fase 1 (Habilitação/Classificação)

5.4.1. O julgamento de Habilitação é **eliminatório**.

5.4.2. Será considerada INABILITADA a INTERESSADA que deixar de apresentar qualquer documento exigido nas subseções 5.2 ou 5.3.
5.4.3. Será considerada HABILITADA a INTERESSADA que cumprir integralmente os requisitos documentais das subseções 5.2 e 5.3.

5.4.3. Dos Critérios de Classificação (Fase 1)

5.4.3.1. O julgamento da segunda etapa da Fase 1 é **classificatório** e se baseará unicamente na pontuação e critérios definidos no **ANEXOS III, IV e V**.

5.4.3.2. A Comissão de Seleção analisará as Propostas de Modelo de Negócio e atribuirá pontuação de 0 (zero) a 100 (cem) pontos, com base nos critérios e pesos definidos nos **ANEXOS III, IV e V**.

5.4.3.3. Os critérios de avaliação avaliarão, no mínimo:
a) Potencial da solução e alinhamento estratégico com os objetivos da PRODAM-SP e da Administração Pública em geral, que poderá ser beneficiária da ferramenta;
b) Viabilidade e maturidade do modelo de negócio da solução proposta.
c) Modelo Financeiro, projeções de investimento e Estratégia Comercial.
d) Estimativa de receitas para a PRODAM-SP e para o Parceiro, incluindo a proposta de compartilhamento de resultados.
e) Estrutura de Governança da Parceria e Gestão de Riscos.

5.4.4. Em caso de empate, serão seguidos os seguintes critérios de desempate:
a) A INTERESSADA que apresentar maior pontuação nos critérios do **Anexo V (Planilha de Capacidade Técnica do Parceiro)**;
b) A INTERESSADA que apresentar maior pontuação nos critérios do **Anexo IV (Planilha de Requisitos Técnicos da Solução e Critérios de Pontuação)**;
c) Na eventualidade de persistência do empate, será realizado sorteio.

5.4.5. Durante a avaliação da documentação da Fase 1, a PRODAM poderá realizar diligências para saneamento de defeitos e/ou solicitação de esclarecimentos, observando o princípio da isonomia.

5.5. Da Publicação do Resultado Provisório da Fase 1

5.5.1. A PRODAM-SP publicará no Sítio de Publicação a lista das INTERESSADAS, indicando seu status como "Habilitada" ou "Inabilitada" e sua respectiva Classificação Provisória.

5.5.2. Da decisão de habilitação e classificação caberá Recurso Administrativo, nos termos da Seção VII.

SECÃO VI - DA PROVA DE CONCEITO (POC)

6.1. Da Realização da Prova de Conceito (POC) (Análise Prática)

6.1.1. As INTERESSADAS que tiverem sua documentação aprovada e estiverem classificadas até o 3º (terceiro) lugar na Fase 1 serão convocadas, por e-mail, para a realização da Prova de Conceito (POC).

6.1.2. A POC será realizada no local designado pela PRODAM-SP, em período agendado pela Comissão.

6.1.2.1. A INTERESSADA fica ciente de que a Prova de Conceito (POC) poderá ocorrer em município diverso da sede da PRODAM, uma vez que a parceria que se visa formular objetiva a prestação de serviços em todas as unidades da federação.

6.1.3. A INTERESSADA deverá providenciar, às suas expensas, todos os equipamentos de informática, *softwares*, sistemas operacionais, bancos de dados, licenças e demais recursos necessários para as comprovações dos requisitos funcionais de sua solução, conforme **ANEXO II**.

6.1.4. As aplicações e sistemas necessários para a POC deverão estar previamente instalados e funcionais nos equipamentos a serem disponibilizados pela INTERESSADA. A PRODAM-SP será responsável somente pela disponibilização do espaço físico, instrumentos jurídicos com os municípios e demais elementos que dependam de negociações com o Poder Público.

6.1.5. Falhas que venham a ocorrer no momento da realização da POC (falhas de *software*, *hardware* ou configuração do ambiente da INTERESSADA) serão de responsabilidade da proponente.

6.1.6. O não cumprimento da Prova de Conceito no período estabelecido, ou a impossibilidade de realização dos testes por falha nos equipamentos da INTERESSADA, implicará em sua inabilitação sumária.

6.1.7. Será permitido o acompanhamento da POC pelas demais INTERESSADAS, entretanto, não será permitido que estas expressem comentários, manifestações ou discordâncias durante os testes. Eventuais manifestações deverão ser realizadas por meio de recurso, nos termos da Seção VII.

6.1.8. Durante a realização da Prova de Conceito – POC, caso seja constatada característica incompatível com a documentação apresentada na fase anterior, a nota provisoriamente atribuída poderá ser revista, mediante a devida justificativa.

6.2. Da Publicação do Resultado Final (Fase 2)

6.2.1. As propostas serão julgadas da seguinte forma:

a) Obterão o resultado "NÃO ATENDE" na Prova de Conceito (POC), conforme os critérios de avaliação obrigatórios definidos no ANEXO II. O não atendimento a um ou mais requerimentos definidos como obrigatórios no ANEXO II resultará na desclassificação.

b) Obterão o resultado "ATENDE" na Prova de Conceito (POC), validando o atendimento a 100% (cem por cento) dos requisitos obrigatórios definidos no ANEXO II.

6.2.2. O Resultado Final da Fase 2 (Julgamento) será publicado no Sítio de Publicação.

6.2.3. Dessa decisão caberá Recurso Administrativo, nos termos da Seção VII.

SEÇÃO VII - DOS RECURSOS ADMINISTRATIVOS

7.1. O presente Edital prevê duas fases recursais distintas, uma para cada fase do processo seletivo.

7.2. Do Recurso da Fase 1 (Habilitação/Classificação):
7.2.1. Após a publicação do resultado provisório da Fase 1 (item 5.5), poderá ser apresentado recurso administrativo no prazo de 05 (cinco) dias úteis contados de sua publicação, contra a decisão da Fase 1.

7.3. Do Recurso da Fase 2 (Julgamento):
7.3.1. Após a publicação do resultado da Fase 2 (item 6.2), poderá ser apresentado recurso administrativo no prazo de 05 (cinco) dias úteis contados de sua publicação, contra a decisão da Fase 2.

7.4. Interposto o recurso administrativo (seja da Fase 1 ou Fase 2) por uma das INTERESSADAS, o documento será publicado no sítio informado no preâmbulo para vista das demais.

7.5. Das razões do recurso administrativo, poderá ser interposta contrarrazões pelas demais, no prazo de 05 (cinco) dias úteis contados de sua publicação.

7.6. A interposição de recurso e de contrarrazões deverá ser realizada exclusivamente para o endereço eletrônico informado no preâmbulo, devidamente fundamentada e motivada, não sendo conhecidas as interposições efetuadas após os prazos legais, bem como as ausentes de motivação e fundamentação.

7.7. A PRODAM-SP decidirá os recursos e as contrarrazões no prazo de 5 (cinco) dias úteis, a contar do dia útil imediatamente posterior ao do término do prazo de interposição das INTERESSADAS.

7.8. Realizada a análise das razões e contrarrazões, a área responsável poderá reconsiderar sua decisão, ou, no caso de manutenção da decisão, encaminhar o recurso à Autoridade Superior para decisão final.

7.9. A decisão do recurso administrativo, das contrarrazões e do resultado final (de cada fase) será publicada no sítio informado no preâmbulo.

SEÇÃO VIII - DA CONVOCAÇÃO E AVALIAÇÃO DE INTEGRIDADE

8.1. Da Convocação

8.1.1. Após a disponibilização da classificação final da Fase 2 e o julgamento de todos os recursos, a PRODAM-SP convocará a INTERESSADA mais bem classificada.

8.1.2. As demais empresas habilitadas e classificadas comporão o Cadastro Reserva, que permanecerá vigente por 12 (doze) meses, facultando à PRODAM-SP convocá-las, seguindo a ordem de classificação, segundo seus critérios de conveniência e oportunidade.

8.2. Da Avaliação de Integridade (Due Diligence)

8.2.1. Convocada, a INTERESSADA será submetida pela PRODAM-SP à Avaliação de Integridade (*Due Diligence*), conforme previsto nas normas internas da PRODAM-SP e da Prefeitura de São Paulo, e a sua recusa implicará em sua imediata desclassificação.

8.2.2. A avaliação de integridade será realizada utilizando-se de formulário específico, com a finalidade de reunir informações sobre o perfil e a reputação da empresa e dos seus representantes, sócios e administradores, assim como verificar a adoção de mecanismos e procedimentos de integridade voltados à prevenção e ao combate à fraude e à corrupção, dentre outras.

8.2.3. O formulário será encaminhado por correio eletrônico ao representante indicado na proposta, devendo ser preenchido no prazo máximo de 5 (cinco) dias úteis contados de seu recebimento.

8.2.4. A PRODAM-SP poderá solicitar, a qualquer momento, esclarecimentos adicionais ou documentos para subsidiar sua análise, cabendo a INTERESSADA atender no prazo máximo de 05 (cinco) dias úteis contados de cada solicitação.

8.2.5. A INTERESSADA será informada do resultado da sua avaliação de integridade quando o Grau de Risco de Integridade (GRI) apurado for baixo ou médio, ficando ciente de que poderá estar sujeita a atender a controles de mitigação de riscos.

8.2.6. A INTERESSADA será informada do resultado da sua avaliação de integridade quando o Grau de Risco de Integridade (GRI) apurado for alto, ficando ciente de que esse risco poderá implicar em sua desclassificação e, consequentemente, a não celebração da parceria, situação em que a PRODAM-SP selecionará a próxima INTERESSADA da lista de classificação.

8.2.7. As informações coletadas durante a avaliação de integridade serão consideradas sigilosas, sendo vedada a divulgação e o acesso por terceiros, salvo o disposto nos itens 8.2.5 e 8.2.6.

SEÇÃO IX - DA CELEBRAÇÃO DA PARCERIA

9.1. A empresa convocada deverá celebrar o Termo de Confidencialidade com a PRODAM-SP, visando proteger informações relevantes conforme a legislação aplicável.

9.2. O **ANEXO VI** deste edital consiste na minuta-padrão de Contrato Associativo, devendo a sua construção ser negociada entre a PRODAM-SP e a convocada antes de sua formalização, excetuando-se o que for vedado pela lei, por princípios da Administração Pública e pelo Regulamento de Parcerias em Oportunidades de Negócio da PRODAM-SP.

9.3. A recusa injustificada da convocada em celebrar o Termo de Confidencialidade ou o Contrato de Parceria implicará em sua imediata desclassificação.

9.4. Celebrado o contrato de parceria, as PARTES devem elaborar o Plano de Negócio final, documento que se destina a descrever os objetivos da oportunidade de negócio e quais passos devem ser dados para que esses objetivos sejam alcançados, levando em consideração a proposta apresentada (ANEXO III) e contendo prazos e instâncias de aprovação.

SEÇÃO X - DAS DISPOSIÇÕES GERAIS

10.1. Todos os documentos relacionados a esse chamamento público deverão ser enviados exclusivamente ao endereço eletrônico informado no preâmbulo deste edital.

10.2. O teor, a integridade, a autenticidade e a veracidade dos documentos enviados serão de responsabilidade da participante, que responderá nos termos da legislação civil, penal e administrativa por eventuais fraudes.

10.2.1. Todos os documentos enviados em idioma diferente do português, deverão ser acompanhados de traduções, simples ou juramentadas.

10.3. A PRODAM-SP poderá, a qualquer momento, conferir e solicitar documentos complementares para sanar dúvidas ou eventuais falhas encontradas na documentação apresentada, bem como realizar eventuais diligências, observando o princípio da isonomia.

10.4. Todos os dados pessoais obtidos em razão dos procedimentos estabelecidos nesse edital serão tratados à luz da Lei Geral de Proteção de Dados Pessoais (LGPD).

10.5. Fica designada Comissão Especial para Seleção de Parceiro Privado, com competências para o planejamento, processamento e gestão deste chamamento.

10.6. É de responsabilidade das INTERESSADAS informar e manter atualizado o seu endereço eletrônico institucional que servirá de contato pela PRODAM-SP em todo o procedimento.

10.7. As INTERESSADAS arcarão com todos os custos decorrentes de sua participação neste chamamento público, incluindo, mas não se limitando, aos custos de preparação de documentação e realização da Prova de Conceito (POC).

10.8. A autoridade competente poderá, a qualquer tempo, revogar o presente chamamento por razões de interesse público decorrente de fato superveniente devidamente comprovado, ou anulá-lo por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado.

10.9. O processo de seleção de parceiro privado é público, de modo que será dada publicidade aos documentos e dados apresentados pelas INTERESSADAS em suas Propostas, as quais ficarão responsáveis pelo encaminhamento de documentos e dados necessários apenas à finalidade do processo. A PRODAM não se responsabiliza pelos efeitos da publicidade dos dados, inclusive pessoais, não relacionados à finalidade do processo, mas, ainda assim, enviados pelas INTERESSADAS.

10.10. Na contagem dos prazos estabelecidos neste edital e seus anexos, o dia do início é excluído e o dia do vencimento é incluído. Só se iniciam e vencem os prazos em dias de expediente na PRODAM.

10.11. Modificações no edital e seus anexos serão divulgados pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido para recebimento das propostas será recontado, exceto se a alteração não afetar a sua formulação, resguardando, em qualquer caso, o tratamento isonômico às interessadas.

10.12. A PRODAM responderá às INTERESSADAS sobre a decisão dos pedidos de esclarecimentos, impugnações e recursos, pelo endereço eletrônico utilizado para o encaminhamento e publicará no sítio informado no preâmbulo deste edital, estes e os demais atos para conhecimento geral.

10.13. As questões não previstas neste edital e seus anexos serão solucionadas pela PRODAM-SP, de ofício ou por provocação das INTERESSADAS, sempre mediante interpretação que privilegie os princípios constitucionais e os da Lei nº 13.303/2016.

SEÇÃO XI - DO FORO

11.1. Os litígios relacionados ao processo a que se refere este edital e seus anexos serão resolvidos pelo foro da Comarca de São Paulo, ressalvada a hipótese de outra solução negociada em contrato.

São Paulo, __ de _____ de 2026.

_____	_____
NOME DA AUTORIDADE COMPETENTE	**NOME DA AUTORIDADE COMPETENTE**
CARGO DA AUTORIDADE COMPETENTE	**CARGO DA AUTORIDADE COMPETENTE**

ANEXOS DO EDITAL PRODAM:

ANEXO I: Plano de Negócio Preliminar da Oportunidade
ANEXO II: Roteiro e Critérios de Avaliação da Prova de Conceito (POC)
ANEXO III: Requisitos da Proposta
ANEXO IV: Planilha de Requisitos Técnicos da Solução e Critérios de Pontuação
ANEXO V: Planilha de Capacidade Técnica do Parceiro
ANEXO VI: Minuta-padrão de Contrato Associativo (Anexos A, B, C, D e E)
ANEXO VII: Declaração de Transação com Parte Relacionada
ANEXO VIII: Declaração de Ausência de Impedimento para Contratar com a PRODAM-SP

EDITAL DE CHAMAMENTO PÚBLICO PARA SELEÇÃO DE PARCEIRO PRIVADO	
Edital Nº XXXXXXXXXXXX	Objeto Monitoramento e Análise Avançada de Imagens para a Segurança Pública Municipal
ANEXO I – PLANO DE NEGÓCIO PRELIMINAR DA OPORTUNIDADE	

PLANO DE NEGÓCIO PRELIMINAR DA OPORTUNIDADE – PNPO

SOLUÇÃO DE MONITORAMENTO E ANÁLISE AVANÇADA DE IMAGENS PARA A SEGURANÇA PÚBLICA MUNICIPAL

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

ÍNDICE

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo

Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP

/ProdamSP

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

1. Proposta de Oportunidade de Negócio

De início, importa esclarecer que o presente plano de negócio não é exauriente e se limita à conveniência e à viabilidade da oportunidade de negócio "Monitoramento e Análise Avançada de Imagens para a Segurança Pública Municipal" em razão da avaliação dos resultados obtidos na cidade de São Paulo em curto período, das projeções iniciais de mercado e da clara convicção da sintonia da missão institucional da PRODAM com a disseminação de boas experiências para os diversos municípios brasileiros interessados. Deixando, portanto, claro o caráter preliminar e norteador, visando a clareza sobre a finalidade da parceria, sem se esgotar exaurir a possibilidade de alterações e versionamento orientados à evolução deste plano de acordo com o escopo pretendido e as necessidades que surgirem ao longo da execução.

1.1. Do Contexto Da Contratação Original (Programa Smart Sampa)

A implantação do Programa Smart Sampa pela Prefeitura de São Paulo, por meio da Secretaria Municipal de Segurança Urbana (SMSU), atendeu a uma diretriz estratégica formalizada no Plano de Metas 2021-2024. Especificamente, a Meta 30, sob o eixo "SP Segura e Bem Cuidada", estabelecia o objetivo de "Integrar 20.000 câmeras de vigilância até 2024".

A justificativa para a contratação, conforme detalhado no Termo de Referência original (Processo SEI Nº 6029.2021/0015253-1), baseou-se também na necessidade de dar continuidade e evoluir programas anteriores (como o City Câmeras) e de cumprir a Lei de Governo Digital (Lei nº 14.129/2021). Esta lei orienta a Administração Pública a estruturar processos de tomada de decisão e promover a cooperação e interoperabilidade entre seus órgãos.

Diferentemente da parceria para internalização ora proposta pela PRODAM, o modelo de contratação original adotado pela SMSU foi o de Pregão Eletrônico. O objeto licitado foi a "Contratação de serviço de vídeo monitoramento, com o fornecimento de toda a estrutura de equipamentos e mão-de-obra necessária para disponibilização, tratamento e armazenamento das imagens a serem capturadas". Esta licitação resultou na contratação de um consórcio privado para operar a plataforma de software e fornecer os equipamentos.

Concomitantemente, a Prefeitura lançou um Edital de Chamamento Público para que empresas privadas e concessionárias pudessem compartilhar voluntariamente as imagens de suas próprias câmeras. Este modelo de adesão permitiu a rápida expansão do programa, através de parcerias e a integração de câmeras.

Este modelo inicial, focado na contratação de um serviço gerenciado por terceiros, foi a solução encontrada pela Prefeitura de São Paulo para implantar rapidamente a infraestrutura de captação de imagens. É exatamente o sucesso dessa captação em larga escala que agora gera a demanda por uma plataforma analítica mais robusta, sob governança pública e soberania municipal, objeto da presente justificativa da PRODAM.

2. DA OPORTUNIDADE DE NEGÓCIO E O INTERESSE PÚBLICO ASSOCIADO

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

2.1. Contextualização da Demanda (A Necessidade da Administração Pública)

A Segurança Pública tem se consolidado como um dos eixos centrais de maior complexidade e demanda por parte da população dos Municípios brasileiros. Esse novo cenário impacta diretamente a percepção de segurança do cidadão, exigindo do Poder Público Municipal uma resposta tecnológica, ágil e baseada em inteligência.

Em resposta a este desafio, a Prefeitura de São Paulo, por meio da Secretaria Municipal de Segurança Urbana (SMSU), implementou o Programa Smart Sampa. Este programa representa, atualmente, o maior sistema de monitoramento da América Latina, tendo atingido a marca de 40.000 câmeras integradas em 2025. O Smart Sampa já demonstrou resultados operacionais expressivos, viabilizando, com o uso de tecnologias como o reconhecimento facial, a captura de mais de 2.335 foragidos da justiça e a realização de mais de 3.625 prisões em flagrante delito.

O próprio sucesso e a expansão exponencial da captação de dados – 40.000 feeds de vídeo contínuos – geraram um desafio operacional de segunda ordem: a impossibilidade fática de monitoramento e análise humana reativa ou proativa de tal volume de informação. A infraestrutura de câmeras, um investimento público de grande envergadura, encontra-se em um ponto de inflexão onde sua eficácia máxima só pode ser atingida com a aplicação de uma camada robusta de inteligência artificial (IA) e análise de vídeo avançada.

Esta "necessidade" foi expressamente reconhecida pela Administração Pública. As Prefeituras de diversas partes do país têm buscado ativamente a PRODAM para conhecer novas soluções tecnológicas, incluindo o uso de Inteligência Artificial, visando apoiar suas operações diárias e ampliar a eficiência de suas políticas integradas.

Portanto, a oportunidade de negócio que se apresenta não é a de criar um sistema de vigilância do zero, mas de potencializar o investimento público já realizado. A demanda crítica é pela identificação e, fundamentalmente, pela utilização de uma plataforma analítica capaz de transformar o repositório massivo de imagens em inteligência acionável e soberana para o Município.

2.2. O Posicionamento Estratégico da PRODAM (O Agente GovTech)

A Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo (PRODAM), criada pela Lei Municipal nº 7.619 de 1971, é a GovTech da Prefeitura de São Paulo. Seu objeto social e suas atribuições institucionais a posicionam como o braço tecnológico e o executor preferencial das políticas de Tecnologia da Informação e Comunicação (TIC) da Administração Municipal.

A PRODAM não se limita a um papel de mero processamento de dados. A empresa possui e opera a infraestrutura crítica de TIC do Município, incluindo um Data Center robusto em capacidade de armazenamento e serviços avançados de segurança cibernética, como Security Operations Center as a Service (SOCaaS) e Web Application Firewall (WAF). A empresa é, ainda, parceira estratégica da Secretaria Municipal de Inovação e Tecnologia (SMIT) e da Secretaria de Gestão (SEGES) na execução do Plano Estratégico de Transformação Digital da Cidade.

A PRODAM-SP também reforçae se consolida como um pilar estratégico na modernização da gestão e dos negócios da administração pública, apresentando uma robusta capacidade de entrega construída a partir de um modelo híbrido de desenvolvimento de software. A empresa alia o domínio técnico de seu corpo interno de especialistas, arquitetos de soluções e desenvolvedores à expertise em governança para o gerenciamento de fábricas de software terceirizadas, garantindo escalabilidade e inovação constante. Por meio de metodologias ágeis e padrões rigorosos de qualidade, a companhia atua tanto na execução direta de projetos críticos quanto

na coordenação de parceiros externos, assegurando que as soluções atendam com precisão às demandas complexas da metrópole. Essa dualidade operacional permite à PRODAM integrar tecnologias emergentes e manter sistemas legados com alta disponibilidade, transformando desafios administrativos em serviços digitais eficientes e centrados no cidadão paulistano.

Alinhada às práticas mais modernas de GovTechs federais, como o SERPRO, a PRODAM vem adotando um posicionamento estratégico de "orquestradora de soluções". Conforme demonstrado em lançamentos recentes, a empresa busca atuar como integradora, firmando parcerias com grandes players de mercado (como Amazon Web Services, Google e Microsoft) para ofertar à Prefeitura de São Paulo e às Administrações Públicas em geral, as soluções mais modernas e competitivas.

Neste contexto, a busca por uma parceria estratégica fundamentada no Art. 28, § 3º, inciso II, da Lei 13.303/2016, é o exato cumprimento da missão institucional moderna da PRODAM: atuar como o hub tecnológico que identifica a necessidade do seu cliente e modela uma "oportunidade de negócio" para supri-la com agilidade e segurança jurídica.

2.3. Desafios a serem enfrentados

Ao decidir estrategicamente participar desse mercado com a disseminação da profunda experiência construída ao longo de mais de 50 anos, a PRODAM reconhece e assume os desafios abaixo listados com o a certeza de que a missão institucional promove e exige a intensa participação na transformação digital da Cidade de São Paulo e de todas as outras cidades brasileiras, sempre com responsabilidade estratégica, inovação tecnológica e foco na experiência do cidadão e na melhoria da qualidade de vida nas cidades.

Entre os principais desafios, destacam-se:

- **Alcançar cidades diversas**: Estar ao alcance de cidades distintas e de seus governantes com a capacidade – o quanto possível - de se adequar a cenários locais e específicos.
- **Oferecer a expertise construída ao longo de sua existência**: Colocando seu portfólio de soluções, especialidade e competências a serviço da Gestão Municipal em geral, atribuindo às cidades interessadas agilidade, maturidade e consistência na adoção tecnológica pretendida.
- **Colaborar com o enfrentamento das questões de Segurança Pública**: Oferecer com agilidade, maturidade e expertise soluções tecnológicas de ponta que orientem e colaborem com o enfrentamento das questões da segurança pública e suas visíveis e conhecidas consequências.
- **Melhorar a capacidade de resposta em tempo real**: Em situações emergenciais ou de grande repercussão, é essencial que os governos consigam reagir com agilidade, precisão e eficácia em favor de toda a população ou conviventes no ambiente urbano.
- **Garantir segurança, privacidade e conformidade legal**: Atuando com responsabilidade no uso de dados para personalização das decisões e operações cotidianas, entendendo ser indispensável garantir total aderência à LGPD e a outras normas de proteção de dados, assegurando transparência, controle e confiança por parte dos cidadãos e atores.
- **Oferecer uma experiência positiva, sistêmica e acessível ao cidadão**: Oferecendo dados sobre os benefícios alcançados tanto no limite do município quanto na relação com municípios vizinhos, com o estado e com o governo federal em nome de uma substancial melhoria no atendimento e enfrentamento das questões da segurança pública.
- **Construir uma solução em parceria com o setor privado**: A implementação da solução demanda uma estrutura tecnológica sofisticada e conhecimento especializado, atuação em rede e colaboração. O desafio é encontrar um parceiro com capacidade técnica, visão estratégica e disposição para construção

conjunta de uma solução escalável, interoperável e de alto impacto social, respeitando os limites orçamentários e as diretrizes do setor público.

3. Público-alvo

Municípios brasileiros diversos que busquem soluções tecnológicas baseadas em Inteligência Artificial e operacional no enfrentamento das questões de Segurança Pública no âmbito municipal, com a efetiva integração de dados e informações com os entes estadual e federal.

3.1. Escopo da solução

O Projeto Smart Sampa é uma iniciativa estratégica da Prefeitura de São Paulo para modernizar a gestão pública e a segurança municipal através de uma Plataforma Modular Web integrada.

Escopo Genérico e Resumido:

O escopo inicial e central do projeto está focado na Segurança Pública, visando cumprir a Metas de Plano de Metas Municipais. O objetivo é ir além do monitoramento passivo, transformando a cidade mais segura e eficiente através do uso efetivo de tecnologias digitais e inteligência artificial.

Soluções Smart Sampa:

A solução tecnológica Smart Sampa consiste na implantação de um sistema robusto de videomonitoramento equipado com analíticos avançados de vídeo, que incluem funcionalidades baseadas em Inteligência Artificial (IA), como reconhecimento facial, leitura automática de placas de veículos (OCR) e monitoramento de perímetro.

A plataforma é concebida para ser um sistema de comando e controle, integrando módulos gerenciais de operação, como o Módulo de Atendimento e Despacho (OMS/CAD). Este módulo permite o rastreamento georreferenciado e o empenho eficiente dos agentes de segurança mais próximos às ocorrências, otimizando o tempo de resposta.

A execução do projeto pela PRODAM busca ser realizada por meio de uma Parceria Estratégica fundamentada na Lei nº 13.303/2016, que tem como pilares a internalização de know-how, compartilhamento de tecnologia e a garantia da soberania de dados do Município, mitigando riscos de vendor lock-in.

Este modelo estabelece a base tecnológica para que a plataforma Smart Sampa possa se expandir futuramente para outras áreas vitais da cidade, como tráfego e saúde, promovendo a cooperação e interoperabilidade entre órgãos municipais.

3.2. Funcionalidades estruturantes da solução

I. Plataforma Modular Web e Integração

Plataforma Web Modular: A solução será entregue como uma Plataforma Modular Web, que serve como o hub central de comando e controle. Sua natureza modular garante que o sistema possa ser expandido de forma fluida para integrar novos serviços (como tráfego e saúde) além da segurança pública.

Integração de Câmeras: Cada instância da plataforma deve suportar, no mínimo, 40.000 câmeras por cidade contratada, garantindo o monitoramento isolado entre municípios.

II. Analíticos Avançados de Vídeo (Inteligência Artificial)

A plataforma será equipada com recursos avançados de analíticos de vídeo para transformar o monitoramento passivo em vigilância proativa e inteligente:

Reconhecimento Facial: Permite a identificação automática de indivíduos, útil para buscas em bancos de dados de pessoas desaparecidas ou procuradas pela justiça.

Leitura Automática de Placas (OCR/LPR): Funcionalidade para reconhecimento de placas de veículos em tempo real, crucial para monitoramento de roubo de veículos e identificação de carros envolvidos em ocorrências.

Monitoramento de Perímetro/Cerca Virtual: Detecção de intrusão e movimentos em áreas restritas ou de interesse, disparando alertas automáticos.

Busca Forense Inteligente: Permite a busca rápida e eficiente em grandes volumes de vídeo gravado, usando critérios específicos (como cor de roupa, tipo de veículo, ou direção de movimento), acelerando a investigação de incidentes.

III. Gerenciamento de Ocorrências e Despacho

Solução de Atendimento e Despacho (CAD/OMS): É o sistema gerencial de operação, que centraliza o recebimento, registro e tratamento de ocorrências.

Georreferenciamento e Rastreamento de Agentes: Exibe os agentes de segurança no mapa, em tempo real, com sua posição geográfica.

Recomendação e Empenho de Agentes: O sistema recomenda e permite o empenho dos agentes mais próximos ao endereço da ocorrência, indicando a distância, o que otimiza o tempo de resposta das equipes.

Cronologia de Ocorrências: Permite consultar o histórico detalhado (log) de todas as ocorrências registradas e tratadas na plataforma.

3.3. Monitoramento e análise de desempenho em tempo real

O cerne da modernização da segurança pública urbana reside no monitoramento em tempo real possibilitado pela Plataforma Smart Sampa. A capacidade de integrar e visualizar milhares de câmeras simultaneamente é multiplicada pela importância estratégica da Inteligência Artificial (IA). Ao invés de depender de operadores para analisar passivamente todos os fluxos de vídeo, a IA, por meio de analíticos avançados (como reconhecimento facial e OCR de placas), identifica automaticamente comportamentos ou eventos anômalos. Isso gera alertas proativos e precisos, transformando o videomonitoramento reativo em uma ferramenta de prevenção ativa. O ganho operacional é direto: a IA permite que o Módulo de Atendimento e Despacho (CAD) utilize o georreferenciamento para recomendar e empenhar o agente de segurança mais próximo, reduzindo drasticamente o tempo de resposta e maximizando a eficácia da atuação da segurança pública municipal.

A plataforma ainda proporciona, por meio do módulo de Machine Learning (aprendizagem de máquina), criar novos padrões de monitoramento usando descritivos, algoritmos ou análises de situações capturadas pelas câmeras e dispositivos IoT.

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

3.4. Suporte à territorialização de políticas públicas

Uma das grandes vantagens da Plataforma Smart Sampa e seus analíticos avançados está na capacidade de oferecer segmentação de dados e inteligência analítica para a criação de estratégias operacionais na segurança pública urbana. Ao centralizar o registro de ocorrências e os dados de videomonitoramento, o sistema permite que gestores de segurança segmentem informações de forma granular por período (identificando picos de criminalidade por hora ou dia da semana), eventos específicos (como grandes aglomerações ou manifestações) e delimitação de áreas geográficas (focos de risco em bairros ou zonas de maior incidência). Essa facilidade de filtrar, cruzar e visualizar dados históricos e em tempo real – por meio da Busca Forense Inteligente e dos relatórios gerenciais – capacita as forças de segurança a alocarem recursos de maneira preditiva, planejar rotas de patrulhamento de forma mais eficiente e desenvolver estratégias de prevenção direcionadas, promovendo um uso mais inteligente e otimizado do efetivo municipal

3.5. Características gerais e especificações técnicas da solução

As principais características arquiteturais e conceituais da solução Smart Sampa e do modelo de parceria são:

Plataforma Modular Web: A solução é concebida como uma Plataforma Modular Web, indicando uma arquitetura escalável e flexível que permite a adição e integração de novos sistemas e serviços (como saúde, tráfego, etc.) além do escopo inicial de segurança pública.

Gestão de Ativos e Inventário: O sistema inclui um módulo de gerenciamento de infraestrutura para monitorar, em tempo real, o status de câmeras, links de transmissão, sensores e hardware. Isso garante a alta disponibilidade da solução e a rápida detecção de falhas em qualquer componente da arquitetura.

Sistema de Comando e Controle (C2): O coração da operação é um sistema que integra videomonitoramento e sistemas gerenciais de operação, como o Módulo de Atendimento e Despacho (CAD), funcionando como um hub central para gestão de incidentes.

Baseada em Analíticos de Vídeo (IA): A plataforma exige a implementação de funcionalidades de Inteligência Artificial (IA) para o tratamento e análise das imagens (ex: Reconhecimento Facial, OCR), caracterizando uma arquitetura de Smart Video Analytics.

Integração com Bases de Biometria: A plataforma permite o cruzamento em tempo real de faces capturadas com bancos de dados de procurados e registros criminais. A funcionalidade foca na identificação automatizada de indivíduos com mandados em aberto, gerando alertas instantâneos para o centro de comando.

Georreferenciamento Integrado: O sistema inclui recursos de georreferenciamento para exibir a posição geográfica dos agentes e auxiliar no empenho dos agentes mais próximos às ocorrências, sugerindo uma integração com mapas e serviços de localização.

Modelo de Parceria Estratégica (Compartilhamento de Know-How): O projeto propõe ser implementado por meio de uma Parceria Estratégica, fundamentada no Art. 28, § 3º, inciso II, da Lei nº 13.303/2016.

Foco em Soberania de Dados: O modelo de parceria é escolhido especificamente para garantir a soberania de dados do Município e mitigar o risco estratégico de vendor lock-in (dependência de um único fornecedor), priorizando o compartilhamento do conhecimento entre privado e empresa pública (know-how).

Interoperabilidade e Cooperação: A arquitetura deve promover a cooperação e interoperabilidade entre os órgãos da Administração Pública, bem como entre a base de dados de procurados e o sistema de acompanhamento de funcionamento e conexão das câmeras, alinhada com a Lei de Governo Digital (Lei nº 14.129/2021).

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

3.6. Serviços Oferecidos

A solução proposta não deverá se limitar à disponibilização de uma plataforma tecnológica. Ela deverá ser acompanhada por um conjunto abrangente de serviços que assegurem o sucesso da implantação, a eficiência operacional e a geração de valor contínuo ao longo de todo o ciclo de vida do projeto. Esses serviços serão estruturados para atender às particularidades da administração pública e garantir que cada cliente – independentemente de porte ou nível federativo – seja plenamente apoiado desde a fase de diagnóstico até a operação contínua. A seguir, detalham-se os principais serviços que deverão integrar essa jornada.

A jornada deverá iniciar com o Diagnóstico e a Pré-Vendas, em que a equipe comercial realizará uma reunião inicial com o potencial cliente, apoiada tecnicamente pelos especialistas da solução. Essa etapa tem por objetivo esclarecer dúvidas, demonstrar o funcionamento da plataforma e avaliar a aderência às necessidades institucionais. Caso haja interesse em aprofundar as tratativas, será agendada uma reunião de descoberta para levantar os requisitos técnicos, identificar os riscos e as customizações necessárias, subsidiando o desenho inicial do projeto. Quando aplicável, poderá ser realizada uma Prova de Conceito (PoC), em que a solução seja testada pelo cliente em ambiente controlado por até 90 dias, conforme ajustado com os possíveis clientes, com o acompanhamento próximo aos gestores e pontos de controle periódicos. Ao final da PoC, deverá ser avaliado se os critérios de sucesso foram plenamente atendidos.

Superada essa fase, deverá iniciar a Implantação da Solução, formalizada por meio de um contrato. O processo de implantação deverá iniciar com uma reunião de *kick-off (*uma reunião que apresenta os objetivos, planos, participantes e expectativas de um projeto ou iniciativa*)* entre aPRODAM, o parceiro e o cliente, para alinhar o escopo, arquitetura e cronograma de trabalho. Em seguida, inicia-se a preparação do ambiente, com a configuração da infraestrutura, as integrações com sistemas de identidade e as validações técnicas. O *onboarding (processo de integração e acolhimento de novos funcionários, clientes ou usuários em uma empresa, sistema ou plataforma)* contemplará uma reunião de boas-vindas, orientações de uso e boas práticas para administradores e usuários-chave. Concluída a configuração, ocorrerá o *handover* — isto é, a passagem formal da solução da equipe de implantação para as equipes de operação e suporte — com entrega de documentação, transferência de conhecimento e reunião de transição com o cliente.

A Operação e o Suporte Técnico deverão ser estruturadas em três níveis. O Nível 1 (N1) deverá realizar o primeiro atendimento, registrando e resolvendo incidentes simples ou direcionando chamados mais complexos. O Nível 2 (N2) deverá contar com uma equipe técnica capacitada para fazer as análises aprofundadas e a resolução de problemas mais técnicos, podendo escalar casos ao Nível 3 (N3), o qual deverá reunir especialistas do produto e da área de desenvolvimento, responsáveis por eventuais correções estruturais e soluções específicas. A sustentação deverá ser complementada pela equipe de operações, responsável pela governança técnica do ambiente com monitoramento 24x7, gestão de capacidade, mudanças (GMUD), documentação e conformidade com os padrões de qualidade e segurança.

Além do suporte técnico, deverão ser disponibilizados os Serviços de Consultoria Especializada, que permitirão ampliar os resultados e a aderência institucional da solução. A consultoria poderá incluir integração com sistemas legados, automação de fluxos operacionais, definição de metas e indicadores, segmentação de públicos-alvo, identificação dos canais de comunicação mais eficazes, análise de dados regionais e de participação de influenciadores. Também serão oferecidos serviços voltados à criação de conteúdo estratégico tais como guias, vídeos, publicações para redes sociais e mensagens personalizadas. Esse suporte será contínuo e adaptável a cada realidade, promovendo o maior engajamento e impacto nas ações públicas.

Por fim, a solução proposta deverá contemplar uma oferta robusta de Capacitação, com treinamentos personalizados e modulares. As formações poderão ocorrer de forma online, por meio de sessões ao vivo e

gravadas, ou presencialmente, conforme a necessidade do órgão contratante. Os treinamentos deverão abranger desde o uso básico da ferramenta até funcionalidades avançadas. Todo o conteúdo deverá ser entregue em português, incluindo manuais, tutoriais, FAQs e guias de referência, assegurando que a equipe do cliente esteja apta a utilizar a solução de forma autônoma, estratégica e com foco em resultados.

4. MATRIZ DE RESPONSABILIDADE

4.1. -Matriz de responsabilidades dos parceiros

A solução proposta deverá contemplar não apenas a tecnologia envolvida, mas também um conjunto de serviços estruturantes que garantam a operacionalização, sustentabilidade e evolução contínua.

A seguir, serão apresentadas as responsabilidades associadas às diferentes frentes de atuação preliminarmente previstas no modelo de parceria, e que deverão ser tratadas detalhadamente no contrato associativo:

Item	Serviços	PRODAM	Parceiro	Faturamento	Medição	Horas Ano
1	**INFRAESTRUTURA**					
1.1	Infraestrutura de Hospedagem/Armazenamento	x		medição	Volume e uso	calculadora DIT
1.2	Conectividade inter servidores	x		contagem	links e trechos	projeto
1.3	Gestão da conectividade	x	x	horas/homem	756 horas/mês	9072 horas/ano
1.4	Gestão do contrato operadoras	x	x	contagem	60 horas/mês	720 horas/ano
1.5	Solução de Orquestração Inteligente	x	x	medição	Licença e consumo	escopo
1.6	Instalação, configuração, manutenção, substitutição e sinistralidade das câmeras e dispositivos IoT		x	Incluso no contrato	Percentual do parque instalado	SLA de 95% do tempo total de disponibilidade.
1.7	Componente CDP (Customer Data Plataform)	x	x	medição	Parceiro	Parceiro
2	**SISTEMAS**					
2.1	Integração com outros sistemas	x	x	UST	on demand	on demand
2.2	Gestão de Dados e Perfis	x		Pacote	360 horas/mês	4320 horas/ano
2.3	Customização da Solução e Evolução RoadMap	x	x	UST	on demand	on demand
2.4	Implantação	x	x	UST	on demand	on demand
2.5	Sistema de Gestão de ativos e conteúdo (VMS)		x	Licença de Uso SaaS	Licença e consumo	escopo
2.6	Sistema de reconhecimento facial e padrões (IA e Analytics)		x	Licença de Uso SaaS	Licença e consumo	escopo
2.7	Sistema de Gestão de eventos e despacho de ordens (OMS)		x	Licença de Uso SaaS	Licença e consumo	escopo
2.8	Acesso à Base de Dados biométricos de procurados	x		medição	Parceiro	Parceiro
3	**SERVIÇOS**					
3.1	Gestão de Serviço	x		medição	discriminar serviços	calculadora DIT
3.2	Gestão de Segurança Cibernética	x	x	medição	discriminar serviços	calculadora DIT
3.3	Consultoria/apoio na construção do centro de controle	x	x	medição	Centro Monitor /Adm	consultar
3.4	Atendimento ao cliente nivel 1	x	x	medição	SLA	consultar
3.5	Gestão Contratual (Gestão comercial, gestão do perceiro comercial, gestão da relação com o cliente)	x		Pacote	20 horas/mês	240 horas/ano
3.6	Faturamento	x		Pacote	40 horas/mês	480 horas/ano
3.7	Cobrança	x		Pacote	24 horas/mês	288 horas/ano
3.8	Relacionamento ao cliente	x		Pacote	360 horas/mês	4320 horas/ano
3.9	Consultoria	x	x	horas/homem	167 horas/mês	2000 horas/ano
3.10	Treinamento		x	UST	Parceiro	Parceiro
3.11	Suporte Técnico 1o 2o 3o		x	medição	Parceiro	Parceiro
4	**ATAS DE REGISTRO DE PREÇOS**					
4.1	Câmeras para aquisição	x		contagem	número de câmeras	projeto
4.2	Câmeras como serviço	x		contagem	número de câmeras	projeto
4.3	Marketing e Comunicação Institucional	x		on demand	on demand	on demand
4.4	Conectividade dispositivos externos	x		contagem	links e trechos	projeto

1. INFRAESTRUTURA

1.1. Infraestrutura de Hospedagem/Armazenamento: consiste no fornecimento e manutenção da infraestrutura da solução em ambiente de nuvem pública governamental, assegurando a soberania, a conformidade com exigências legais e a alta disponibilidade.

1.2. Conectividade inter servidores: conexão segura entre os servidores locais da solução e os do data center e nuvem.
1.3. Gestão da conectividade: Monitoramento da disponibilidade, funcionamento, qualidade e interferências indesejadas da conectividade.
1.4. Gestão do contrato operadoras: Monitoramento, avaliação, homologação da qualidade do serviço acordada e comunicação em caso de incidentes ou eventos indesejados.
1.5. Solução de Orquestração Inteligente: refere-se ao motor de decisão que, com base em IA e dados contextuais, coordena de forma automática e integrada os diferentes sistemas da arquitetura do Smart Sampa, definindo fluxos, priorizações e encaminhamentos entre plataformas tecnológicas para garantir operações unificadas e eficientes.
1.6. Componente CDP (Customer Data Plataform): é a base tecnológica que consolida os dados dos cidadãos de forma estruturada e segura, permitindo a construção de perfis únicos e a personalização das interações em tempo real.

2. SISTEMAS

2.1. Integração com outros sistemas: diz respeito ao desenvolvimento e a manutenção de APIs, conectores e protocolos que permitam a interoperabilidade da solução com bases e sistemas já utilizados por entes públicos.
2.2. Gestão de Dados e Perfis: abrange a unificação, a anonimização, o enriquecimento e a atualização dos perfis de cidadãos, com base em dados públicos e privados, visando a maior assertividade e personalização das ações governamentais.
2.3. Customização da Solução e Evolução RoadMap: cobre a adaptação da solução às demandas específicas dos clientes e o desenvolvimento contínuo de novas funcionalidades com base nas prioridades conjuntas da PRODAM e do parceiro.
2.4. Implantação: refere-se à criação e a configuração do ambiente do cliente, a execução do *onboarding* técnico e institucional, a validação de integrações e a disponibilização da solução para uso, conforme o escopo contratado.
2.5. Sistema de Gestão de ativos e conteúdo (VMS): Módulo da solução focado no gerenciamento dos ativos externos (câmeras, sensores e dispositivos de conectividade) verificando em tempo real seu funcionamento, disponibilidade, abrangência, assim também com as imagens geradas atuando na classificação e na decisão sobre armazenamento.
2.6. Sistema de reconhecimento facial e padrões (IA e Analytics): Módulo da solução que reconhece a face e promove a comparação com a base de procurados e desaparecidos conveniada. Baseada em IA, possibilita o aprendizado de máquina (Machine Learning) a fim de reconhecer eventos e movimentos nos espaços urbanos que sejam merecedores de atenção e acompanhamento. Também reconhece placas, objetos e alguns sons.
2.7. Sistema de Gestão de eventos e despacho de ordens (OMS): Módulo da solução que gerencia os bilhetes de alarme, demanda e solicitação de ação enviados para os órgãos competentes. Gerencia eventos, SLAs, respostas e integração com as bases especialistas.
2.8. Acesso à base de dados biométricos de procurados: base de dados de informações biométricas e dados civis de órgãos de segurança pública ou judiciais acessados sob estrita responsabilidade e conformidade com a política de acesso e proteção de dados da PRODAM, disponibilizados exclusivamente para comparação das imagens e faces coletadas pelo sistema.

3. SERVIÇOS

3.1. Gestão de Serviço: refere-se à coordenação de recursos, processos e funções para garantir a qualidade e a continuidade do serviço prestado, incluindo o gerenciamento de incidentes, eventos e problemas com base nas melhores práticas de governança operacional.

3.2. Gestão de Segurança Cibernética: abrange a aplicação de controles de segurança da informação, tais como autenticação forte, criptografia de dados, segmentação de rede e auditorias regulares, assegurando a proteção dos dados e o cumprimento da LGPD.

3.3. Consultoria/apoio na construção do centro de controle: é o ambiente de monitoramento da operação em tempo real, com *dashboards* gerenciais e operacionais que permitam o acompanhamento do desempenho das campanhas, notificações, fluxos e interações.

3.4. Atendimento ao cliente nível 1: é o suporte inicial ao usuário, com foco em resolução de demandas simples ou encaminhamento estruturado aos níveis superiores. Esse serviço é guiado por scripts padronizados e protocolos definidos.

3.5. Gestão Contratual (Gestão comercial, gestão do perceiro comercial, gestão da relação com o cliente): envolve o acompanhamento e controle da execução contratual, garantindo o cumprimento dos direitos e obrigações pactuados com os clientes, além de promover a transparência e a regularidade na relação institucional (ou comercial/contratual), ainda que haja, segundo política própria, a participação de parceria comercial no projeto..

3.6. Faturamento: é o processo de geração de faturas com base na contratação e uso da solução, incorporando eventuais descontos, bônus ou ajustes previstos contratualmente. Garantindo a rastreabilidade e a conformidade contábil.

3.7. Cobrança: refere-se à emissão, o controle e o recebimento dos valores devidos pelos clientes, além da efetivação dos repasses à empresa parceira, conforme modelo de remuneração acordado.

3.8. Relacionamento ao cliente: corresponde ao acompanhamento próximo do cliente, compreendendo as suas necessidades, promovendo o engajamento, monitorando a satisfação e propondo melhorias nas experiências de uso da solução.

3.9. Consultoria: compreende o apoio técnico e estratégico à implementação e à evolução do uso da solução, incluindo o desenho de campanhas, a definição de públicos, a seleção de canais, a produção de conteúdo e a análise de resultados.

3.10. Treinamento: abrange a capacitação de usuários e administradores da solução, por meio de treinamentos presenciais, online, assíncronos e manuais detalhados, garantindo a autonomia e a boa experiência de uso.

3.11. Suporte Técnico 1o 2o 3º: é o conjunto de atendimentos técnicos escalonados conforme a complexidade do chamado. Sendo que o 1º nível atende de forma generalista; o 2º nível atua em falhas intermediárias e configurações; e o 3º nível, com equipe especializada, trata de ocorrências críticas, de correções e de desenvolvimentos pontuais.

4. ATAS DE REGISTRO DE PREÇO

4.1. Câmeras para aquisição: Fornecimento de câmeras e sensores, assim como dos ativos necessários para a devida instalação desses instrumentos por meio de imobilização (CAPEX) entre o cliente e os fornecedores detentores de Atas de Registro de Preços junto à PRODAM.

4.2. Câmeras como serviço: Fornecimento de câmeras e sensores, assim como dos ativos necessários para a devida instalação desses instrumentos por meio de consumo e serviço (OPEX) entre o cliente e os fornecedores detentores de Atas de Registro de Preços junto à PRODAM.

4.3. Marketing e Comunicação Institucional: inclui as campanhas promocionais, o material institucional, as ações em redes sociais, os eventos presenciais ou virtuais, a mídia cooperada e o apoio à divulgação da solução, respeitando a imagem institucional de ambos os parceiros.

4.4. Conectividade dispositivos externos: Instalação e conexão dos meios de conectividade e transmissão de dados por cabo, fibra ou wifi entre servidores e infra da PRODAM e nuvem.

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

4.2. Fornecimento das Câmeras e Sensores

As câmeras e sensores, assim como outros dispositivos necessários captura de imagens e dados no ambiente urbano externo serão fornecidos aos clientes por meio de Ata de Registro de Preços para aquisição ou como serviços, proporcionando a relação agilizada entre a cidade cliente e os fornecedores ou fabricantes de mercado.

Resultados decorrentes da parceria

As receitas decorrentes da Parceria serão originadas de contratos firmados pela PRODAM com os clientes, sendo de sua responsabilidade a arrecadação integral dos valores e a posterior transferência à PARCEIRA das quantias que lhe forem devidas.

Os valores cobrados de cada cliente serão definidos caso a caso, conforme as particularidades de cada contrato.

A PRODAM recolherá os tributos incidentes sobre o valor total recebido, enquanto a PARCEIRA será responsável pelos tributos aplicáveis à sua parte, conforme as legislações federais, estaduais, municipais ou distritais vigentes.

Os repasses à PARCEIRA ocorrerão somente após a efetiva quitação dos valores pelos clientes.

A divisão das receitas observará os percentuais previamente estabelecidos em contrato, inicialmente projetada em 50% para a PRODAM e 50% para a PARCEIRA, calculada sobre a Receita Operacional Líquida.

Essa divisão contratual deverá ter como fundamento a análise das responsabilidades assumidas e das contribuições efetivas de cada parte no desenvolvimento e na sustentação da solução proposta. Ressalta-se, contudo, que os percentuais definidos nesta etapa possuem caráter indicativo, podendo ser ajustados após a consolidação do modelo operacional, da definição detalhada da utilização dos recursos e da apuração final dos custos envolvidos.

Em situações de glosa ou aplicação de multa por parte do cliente, o valor correspondente será deduzido da parcela da parte que tiver dado causa ao prejuízo. Caso não seja possível identificar a parte responsável, o abatimento será realizado de forma proporcional entre as partes.

O modelo de parceria não prevê qualquer aporte financeiro por parte da PRODAM, tampouco remuneração garantida à empresa parceira. O repasse estará condicionado exclusivamente à receita proveniente dos contratos firmados com os clientes da PRODAM, o que implica que a empresa parceira deverá assumir riscos, realizar investimentos próprios e responder pelas responsabilidades inerentes ao desenvolvimento, customização, implantação e a sustentação da solução.

A PRODAM projeta, de forma unilateral e preliminar, que a solução registre um valor financeiro estimado com base no volume de atendimento processado, considerando os disparos realizados, entre R$ 15 milhões e R$ 30 milhões no primeiro ano, podendo alcançar entre R$ 70 milhões e R$ 140 milhões no quinto ano. Trata-se de estimativa indicativa de ordem de grandeza, não vinculante, cujo objetivo é proporcionar às empresas interessadas uma visão antecipada do potencial de uso da solução. Ressalta-se, contudo, que a empresa parceira deverá reunir condições técnicas, operacionais e financeiras para adequar seus recursos conforme a variação da demanda ao longo dos volumes projetados, garantindo escalabilidade e continuidade da oferta.

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

4.3. Mapeamento de riscos

Risco	Definição	Alocação (público, privado ou compartilhado)	Impacto (alto, médio, baixo)	Probabilidade (frequente, provável, ocasional, remota ou improvável)	Mitigação (medidas, procedimentos ou mecanismos para minimizar)
Discrepância com preço de mercado	**Discrepância com preço de mercado** ocorre quando o **preço praticado** para um produto, serviço ou ativo financeiro é **diferente do valor geralmente aceito ou predominante no mercado**.	compartilhado	alto	ocasional	Monitoramento constante do mercado, ajuste de preços flexíveis.
Tecnologias emergentes	Tecnologias emergentes são inovações tecnológicas em estágio inicial de adoção, mas com alto potencial de transformação radical em setores, modelos de negócio e comportamentos. Elas representam novidades que podem mudar a forma como trabalhamos, nos relacionamos e consumimos.	compartilhado	médio	provável	Investimentos em P&D, atualizações constantes da solução.
Concorrência de novas ferramentas	A concorrência de novas ferramentas refere-se à **disputa no mercado que surge com o advento de novas tecnologias e soluções, que desafiam as empresas e métodos existentes**. Essas novas ferramentas podem vir de qualquer direção e, muitas vezes, de onde menos se espera, redefinindo o cenário competitivo de um setor.	compartilhado	alto	provável	Análise competitiva, inovação contínua e diferenciação do produto.
Capacidade de atendimento	Capacidade de atendimento é o **volume máximo de solicitações que uma equipe ou serviço pode processar em um determinado período, sem comprometer a qualidade do atendimento**. Esse conceito envolve não apenas a quantidade de atendimentos, mas também a eficácia na resolução de problemas e a experiência geral do cliente. É a ponte entre o que a equipe pode entregar e o que a demanda dos clientes exige, sendo essencial para o sucesso e a sustentabilidade de um negócio.	compartilhado	médio	ocasional	Planejamento de recursos humanos, treinamento e contratação estratégica.
Reputação e conformidade legal	**Conformidade legal** refere-se ao potencial de perdas devido ao **não cumprimento de leis e regulamentos**, enquanto o **risco de reputação** diz respeito aos danos à **imagem e credibilidade** de uma organização, que muitas vezes são causados por falhas de conformidade.	compartilhado	médio	remota	Programas de compliance, auditorias regulares, transparência nas operações.
Mudanças na Legislação Tributária	Do ponto de vista dos riscos, as **mudanças na legislação** representam os potenciais problemas decorrentes da falha em **cumprir novas leis, regulamentos e normas** que afetam as operações de uma empresa. Esse tipo de risco é classificado como **risco legal, regulatório ou de conformidade**.	compartilhado	alto	ocasional	Revisão entre as partes, com recomposição do reequilíbrio econômico-financeiro do contrato.
Flutuações econômicas	Flutuações econômicas são os ciclos de altos e baixos na atividade econômica de um país, caracterizados por períodos de expansão (crescimento) e recessão (contração). Essas oscilações podem afetar a renda nacional, o emprego, a produção e os preços, e são causadas por fatores variados, como mudanças na oferta e demanda, custos de produção, políticas governamentais e o mercado financeiro.	compartilhado	alto	provável	Estratégias de mitigação de riscos financeiros
Dependência tecnológica	**Dependência tecnológica** refere-se a: **Integração de sistemas**: Se diferentes fornecedores fornecem câmeras, softwares de análise, armazenamento e redes, qualquer falha ou incompatibilidade pode comprometer todo o ecossistema. **Risco de lock-in**: Dependência de tecnologias proprietárias pode dificultar substituições ou atualizações, aumentando custos e reduzindo flexibilidade. **Escalabilidade e manutenção**: Em projetos nacionais, a interoperabilidade é crítica. Se uma empresa não acompanha atualizações ou sai do mercado, isso pode gerar grandes problemas. **Segurança cibernética**: Vulnerabilidades em um fornecedor podem afetar toda a cadeia, ampliando riscos de invasão ou vazamento de dados.	compartilhado	alto	ocasional	Diversificação de tecnologias e fornecedores, planos de contingência.
Questões de Segurança Cibernética	**Questões de segurança cibernética** referem-se a **potenciais ameaças e vulnerabilidades** que podem ser exploradas para causar danos, interrupções ou acesso não autorizado a sistemas e dados digitais. O foco está na probabilidade de um evento adverso ocorrer e no impacto potencial que ele teria sobre a confidencialidade, integridade e disponibilidade das informações. Conjunto de práticas, processos e tecnologias voltados para proteger sistemas, redes e dados contra acessos não autorizados, ataques, danos ou interrupções, garantindo **confidencialidade, integridade e disponibilidade** das informações.	compartilhados	alto	ocasional	Investimento em segurança cibernética, protocolos robustos de proteção de dados.
Mudança nas necessidades do cliente	**Mudanças nas necessidades do cliente** referem-se à ameaça de que os produtos ou serviços de uma empresa se tornem **obsoletos ou menos atrativos** devido à evolução das expectativas, hábitos ou prioridades dos consumidores. Isso pode impactar negativamente o desempenho financeiro, a participação de mercado e a reputação da marca.	compartilhado	alto	ocasional	Pesquisa de mercado e flexibilidade para adaptar os serviços.
Sinistralidade de câmeras, instalações e dispositivos de campo	**A exposição a defeitos de funcionamento e operacionais causados por vandalismo, depredação, ação com propósitos escusos e destruição proposital.**	Parceiros	alto	alta	Pesquisas da taxa de sinistralidade em operações similares. Atuação de mitigação da ação depredatória. Uso de tecnologia e instrumental de proteção aos ativos.

Nas parcerias em oportunidade de negócio, ambas as partes deverão reconhecer a existência de riscos potenciais inerentes à natureza da colaboração e da solução proposta. Compreendendo a importância da gestão eficaz desses riscos para o sucesso da parceria, a PRODAM e a PARCEIRA deverão se comprometer a adotar medidas proativas de mitigação deles.

Esta abordagem deverá incluir a revisão e a atualização regular das estratégias de mitigação para assegurar as suas eficácias e a relevância diante das dinâmicas do ambiente de negócios, da tecnologia envolvida e do mercado.

Além disso, a PRODAM e a PARCEIRA deverão se comprometer com a comunicação aberta e colaborativa, especialmente em relação à gestão de riscos. Qualquer identificação de um novo risco ou a mudança significativa em um risco existente deverá ser comunicada imediatamente entre as partes.

As estratégias de mitigação de riscos deverão ser revisadas anualmente, ou mais frequentemente se necessário, para garantir que continuem alinhadas com as mudanças no cenário de negócios e tecnológicos, ajustando-se para abordar efetivamente quaisquer novos riscos ou mudanças nos riscos existentes.

A PRODAM oferece, unilateral e preliminarmente, matriz de riscos que apresentamos acima.

5. Diretrizes de Governança

5.1. Indicação da necessidade de publicação de extrato de oferta tecnológica

Conforme o § 1º do artigo 6º da Lei nº 10.973/2004 (Que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências), nas hipóteses de contratos de transferência de tecnologia e de licenciamento para outorga de direito de uso ou de exploração de criações desenvolvidas por meio da parceria, não se vislumbra a necessidade de publicação de extrato de oferta tecnológica.

5.2. Indicação da necessidade de contratação de consultorias especializadas

Entende-se que não houve necessidade de contratação de consultoria especializada para o desenvolvimento da parceria proposta, visto que as partes envolvidas deverão possuir expertise, capacidade técnica e conhecimento do mercado suficientes para estruturar os termos e condições da oportunidade de negócio. No entanto, poderá ser indicada a contratação da consultoria em momento posterior do procedimento.

5.3. Da comprovação de inviabilidade de procedimento competitivo

A presente parceria não visa à simples aquisição de produto pronto, mas sim a cocriação e operação conjunta de uma solução integrada com as plataformas da PRODAM, com o compartilhamento dos riscos, dos resultados e das responsabilidades técnicas e operacionais. Trata-se de uma iniciativa que exige a integração sistêmica com a arquitetura já existente, o que inviabiliza contratação tradicional de uma solução “de prateleira”.

A existência de tecnologias similares não impede que a PRODAM, como empresa estatal, opte por desenvolver uma solução própria ou em parceria, especialmente quando envolvido o tratamento de informações sensíveis, a arrecadação e a integração com os sistemas estratégicos do governo federal. Trata-se de um mecanismo legítimo para criar soluções aderentes à realidade regulatória do setor público, sem a dependência de fornecedores externos ou de plataformas proprietárias.

A natureza do objeto envolve a pesquisa, o desenvolvimento, a construção conjunta e a exploração futura de soluções inéditas, não sendo juridicamente licitável no âmbito de uma contratação ordinária, pois não se busca a aquisição de um bem ou serviço padronizado, mas a estruturação de uma nova cadeia de soluções, cujo escopo técnico ainda está em evolução, razão pela qual se justifica a celebração de parceria estratégica com a empresa que demonstre a capacidade técnica, a visão de negócio e o compromisso institucional com os valores públicos envolvidos.

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

Esses elementos, conectados à natureza associativa do contrato, afastam quaisquer interpretações no sentido de eventual desvirtuamento da modelagem jurídica ou tentativa de burla à licitação convencional para a aquisição de serviços ou insumos. Não se trata de mera aquisição de tecnologia ou de serviço padronizado, mas de uma iniciativa de cocriação estratégica que torna impraticável a comparação objetiva entre propostas previamente existentes, pressuposto indispensável para a realização de procedimento competitivo.

Nesse contexto, com base no Regulamento de Parcerias em Oportunidade de Negócios, será realizado o lançamento de Edital de Chamamento Público, permitindo a ampla participação de potenciais interessados que preencham os requisitos mínimos de qualificação técnica e econômico-financeira, prestigiando os princípios da publicidade, da isonomia, da moralidade administrativa e da busca pela melhor solução associativa para o interesse público.

5.4. Do prazo do contrato de parceria

O contrato de parceria terá prazo mínimo de 2 (dois) anos, podendo ser prorrogado por períodos sucessivos, sem limitação temporal, desde que existam projetos ativos previstos no Plano de Negócio da Oportunidade (PNO). Essa previsão garante a continuidade da oferta e a sustentabilidade da parceria ao longo do tempo, proporcionando segurança jurídica e operacional para ambas as partes.

A qualquer momento, o contrato poderá ser rescindido, desde que respeitado o aviso prévio mínimo de 90 dias, a ser comunicado formalmente pela parte interessada. Esse período tem como objetivo permitir o planejamento e a readequação das partes envolvidas, minimizando os riscos operacionais e os impactos aos clientes.

Durante esse prazo de transição, permanece a obrigação de continuidade na prestação dos serviços referentes aos contratos firmados com os clientes, assegurando a estabilidade e a integridade da solução enquanto se providenciam os ajustes necessários.

Em caso de descontinuidade, a PARCEIRA deverá ainda garantir o suporte e a transferência de conhecimento, conforme cronograma e condições a serem previamente estabelecidos, assegurando uma transição ordenada da operação.

Nos casos de rescisão antecipada não justificada, será aplicada uma penalidade correspondente a 12 (doze) vezes o valor da receita líquida média auferida nos últimos 12 (doze) meses anteriores à comunicação da intenção de descontinuidade, salvo disposição em contrário devidamente justificada em comum acordo entre as partes.

O aviso prévio de 90 (noventa) dias também integra o plano de contingência da parceria, permitindo que a PRODAM, dentro desse prazo, possa iniciar um novo processo seletivo para escolha de nova parceira ou ainda, se mais vantajoso, assumir integralmente a operação com investimentos próprios. Como o contrato de receita é celebrado diretamente com a PRODAM, isso garante a continuidade da oferta, inclusive com a eventual substituição do parceiro, sem prejuízo aos clientes atendidos.

5.5. Diretrizes acerca da propriedade da solução a ser desenvolvida

A propriedade intelectual da solução deverá ser tratada no contrato associativo de parceria, considerando as premissas abaixo:

- Propriedade Pré-existente: Todas as partes mantêm os direitos completos e exclusivos sobre a sua propriedade intelectual pré-existente, utilizada ou não no contexto desta parceria. Cada parte será

responsável por suas propriedades intelectuais, garantindo que não infrinjam os direitos de terceiros e serão responsáveis por quaisquer reivindicações ou ações relacionadas a tais propriedades.

- Propriedades Conjuntamente Criadas: Todo know-how, integrações tecnológicas, componentes de software ou quaisquer outras formas de propriedades intelectual geradas conjuntamente no âmbito desta parceria serão de propriedade conjunta de ambas as partes. Ambas as partes têm os direitos de uso, da distribuição e da reprodução dessas propriedades intelectuais, sem quaisquer obrigações de pagar royalties uma à outra.
- Renúncia de Direitos Futuros: com relação à propriedade intelectual gerada conjuntamente, nenhuma delas exercerá quaisquer direitos futuros de cobranças de royalties ou quaisquer outras formas de compensação pela sua utilização, seja no contexto atual ou em futuras aplicações ou parcerias, salvo em acordo entre as partes.

- Marca SMART SAMPA: as partes reconhecem que é uma marca exclusiva da PRODAM e qualquer divulgação ou menção a ela pelo parceiro dependerá de consentimento prévio e expresso da PRODAM

5.6. Diretrizes acerca do código fonte da solução em parceria

A gestão e a custódia do código-fonte da solução desenvolvida no âmbito da parceria serão de responsabilidade da PRODAM, em ambiente seguro e controlado, garantindo a integridade, a confidencialidade e a rastreabilidade de todo o material produzido. Esse modelo assegura que o patrimônio tecnológico gerado ao longo da parceria permaneça sob guarda institucional, com acesso regulamentado, com o versionamento adequado e com trilha de auditoria, mesmo em cenários de eventual modificação na composição da parceria.

A PRODAM deverá manter sempre a última versão **homologada** da solução instalada, garantindo sua operação segura e em conformidade com os padrões técnicos exigidos. A homologação envolverá testes de segurança especializados realizados pelo parceiro antes da disponibilização em ambiente de produção, incluindo SAST (análise estática de segurança do código, executada exclusivamente pelo parceiro em seu repositório proprietário) e DAST (testes dinâmicos em ambiente controlado, simulando ataques externos para identificação de vulnerabilidades).Esses procedimentos visam antecipar os riscos e corrigir as vulnerabilidades de forma preventiva, assegurando que a solução esteja em conformidade com os padrões de segurança da informação, com as boas práticas de desenvolvimento seguro e com as normas exigidas pela Administração Pública , antes de qualquer ativação em ambiente produtivo.

Adicionalmente, os procedimentos de empacotamento e preparação da versão final da solução — incluindo build, consolidação dos componentes e geração do pacote executável — deverão ocorrer em ambiente técnico adequado e previamente acordado entre as partes, observando protocolos de segurança, auditoria e conformidade definidos em conjunto. A PRODAM receberá apenas o artefato final, já validado e pronto para implantação, garantindo integridade, rastreabilidade e aderência às melhores práticas de DevSecOps. Esse fluxo assegura que a versão disponibilizada em produção seja íntegra, testada e segura, preservando a proteção dos ativos digitais e o cumprimento dos requisitos de segurança aplicáveis ao setor público, sem implicar acesso ao código-fonte proprietário do parceiro.

Então deixamos, certa definição da custódia operacional pela PRODAM está alinhada às diretrizes de compliance, governança tecnológica, segurança da informação e soberania digital do Município de São Paulo, reforçando a confiabilidade da solução perante os entes públicos usuários. Mesmo em cenários de rescisão contratual, descontinuidade ou eventos extraordinários, a PRODAM manterá capacidade plena de operação, monitoramento, parametrização, integração e sustentação da solução, assegurando continuidade do serviço e

proteção dos investimentos públicos — sem interferir no núcleo proprietário ou na propriedade intelectual do parceiro.

Alternativamente, poderão ser adotadas outras estratégias técnicas que garantam níveis equivalentes de segurança, rastreabilidade e mitigação de riscos, incluindo arquiteturas híbridas ou modelos operacionais diferenciados. Qualquer alternativa deverá ser previamente analisada e validada pelas instâncias competentes da PRODAM, especialmente pela área de segurança da informação, assegurando aderência às diretrizes internas e aos normativos aplicáveis à Administração Pública, bem como preservação da separação entre governança pública e núcleo tecnológico proprietário do parceiro.

6. Seleção do parceiro privado

6.1. Do procedimento de seleção

A fase de seleção é etapa essencial no processo de formalização da parceria em oportunidade de negócio, concebida para garantir que a escolha da empresa parceira ocorra de forma transparente, objetiva e alinhada com os princípios que regem a atuação da PRODAM.

Para a oportunidade de negócio em tela, deverá ser realizado o procedimento de Chamamento Público para Seleção do Parceiro Privado, entendendo-se ser uma estratégia sólida para salvaguardar e promover a preservação dos princípios constitucionais.

Os critérios e os requisitos a serem utilizados no edital devem cumprir papel central para a classificação das empresas, permitindo distinguir aquelas que, além de apresentarem aderência técnica, demonstrem a efetiva capacidade de atuar conjuntamente com a PRODAM na execução da solução pretendida.

É importante ressaltar que os requisitos funcionais, os de capacidade e os de sustentabilidade previstos no edital não se confundem com o escopo produtivo da solução nem esgotam o plano de negócios. Ou seja, trata-se de critérios de seleção que visam aferir a experiência, a capacidade técnica e a maturidade organizacional das empresas interessadas, de modo a assegurar que a futura parceria seja conduzida com solidez, responsabilidade e compromisso. Ressalte-se, ainda, que os requisitos serão definidos a partir das necessidades estratégicas da PRODAM e deverão considerar as contribuições recebidas por meio do **Chamamento Público nº XXXX/2026**, de forma a conferir maior robustez e aderência às expectativas.

Nesse sentido, as exigências contidas no edital não devem se limitar a uma verificação documental ou meramente formal. Elas deverão abranger dimensões mais amplas, que incluam comprovações de experiência anterior, indicadores de governança, práticas de segurança e privacidade, além de demonstrações da aptidão em compartilhar riscos, responsabilidades e investimentos. A lógica é assegurar que a empresa selecionada possua, desde o início, condições de compor uma relação de cooperação estável com PRODAM, atuando como parceira estratégica e não apenas como prestadora de serviços.

Por fim, cumpre destacar que o procedimento de seleção não representa a definição final do modelo de negócio ou do detalhamento funcional da solução. Esses aspectos serão tratados em fases posteriores, notadamente no plano de negócios definitivo, momento em que serão ajustados elementos como precificação, governança operacional e responsabilidades específicas de cada parte.

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

6.2. Da vedação ou admissibilidade de consórcio

O procedimento de seleção de parceiro privado poderá permitir a participação de consórcios.

Esta decisão baseia-se na natureza da parceria proposta, caracterizada por sua complexidade operacional e pela nítida fragmentação no oferecimento de soluções, que pela própria arquitetura da PRODAM permite o fornecimento de múltiplos entes na configuração da Parceria.

6.3. Da quantidade de parceiros

Assume-se que oportunidade de negócio em tela, marcada por suas especificidades técnicas e por uma arquitetura complexa, será eficazmente atendida através de uma colaboração, ainda que com múltiplos entes como parceiros, na divisão das atividades e responsabilidades.

Portanto, a eficácia e a eficiência da parceria serão maximizadas por meio de uma parceria, constituindo estrutura direta de colaboração, onde a PRODAM e as parceiras serão responsáveis pelas atividades a serem desenvolvidas.

Admite-se, todavia, a manutenção de um cadastro reserva como medida de prudência e gestão de riscos. Essa prática garante a continuidade do projeto em caso de eventual desistência, incapacidade de execução ou descumprimento das obrigações por parte da empresa selecionada, preservando a viabilidade da oportunidade de negócio e assegurando maior agilidade na substituição da parceira, facultando à PRODAM convocar uma empresa, seguindo a ordem de classificação do cadastro de reserva, segundo seus critérios de conveniência e oportunidade.

A vigência do Cadastro Reserva deverá ser de 12 (doze) meses, a contar da publicação do resultado do julgamento final.

Admite-se também, segundo a análise de conveniência e oportunidade realizada pela PRODAM no curso da execução da parceria, a possibilidade de novo chamamento para atendimento de clientes que não possam ser satisfatoriamente atendidos pela parceria decorrente do presente processo.

6.4. Da vedação ou admissibilidade de empresas em recuperação judicial

Levando em conta que a parceria proposta implica o compartilhamento de riscos e investimentos, é imperativo que o edital exclua a possibilidade de participação de empresas em processo de recuperação judicial, de forma a assegurar a participação somente de empresas que estejam em plena saúde financeira e jurídica, sem quaisquer restrições que possam afetar adversamente o desempenho e a entrega dos serviços propostos.

Tal condição é geralmente atribuída a entidades enfrentando significativas limitações de liquidez, além de uma suspensão temporária no cumprimento de obrigações financeiras com credores. Mesmo que essa situação seja temporária, ela pode comprometer a capacidade da parceria de atender com eficiência e pontualidade às demandas dos clientes da PRODAM.

6.5. Da qualificação técnica funcional

6.5.1 Para assegurar que a parceria a ser firmada seja capaz de atender de forma efetiva às demandas do projeto, deverão ser adotados requisitos técnicos funcionais como critério de qualificação das soluções propostas pelas empresas interessadas. Tais requisitos, bem como os pesos e pontuações atribuídas, permitirão avaliar a

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 425 – Centro – CEP: 01009-000 – São Paulo – SP
/ProdamSP

aderência das soluções às especificidades técnicas e operacionais pretendidas, garantindo a viabilidade prática da implementação e a entrega dos resultados esperados.

6.6. Da qualificação técnica de capacidade

6.6.1 Para assegurar que a futura parceira possua experiência prática e estrutura adequada para executar, de forma eficiente e segura, as atividades previstas na parceria, deverão ser adotados requisitos de capacidade técnico-operacional. Tais requisitos, bem como os pesos e pontuações atribuídas, permitirão verificar não apenas a conformidade formal da proposta, mas também a efetiva aptidão da empresa para entregar os resultados pactuados, mitigando riscos de inadimplemento, atrasos ou falhas na execução.

6.7. Da qualificação técnica de sustentabilidade

6.7.1 Para assegurar que a futura parceira esteja alinhada aos princípios ambientais, sociais e de governança da PRODAM, deverão ser adotados requisitos de sustentabilidade. Tais requisitos, bem como os pesos e pontuações atribuídas, permitirão selecionar empresas comprometidas não apenas com a entrega técnica da solução, mas também com a geração de valor socioambiental, a mitigação de impactos negativos e a promoção de práticas transparentes e responsáveis.

6.8. Da proposta econômico-financeira

A proposta econômico-financeira apresentada pelas INTERESSADAS deverá refletir a matriz de responsabilidade e ser acompanhada da planilha de custo detalhada. As INTERESSADAS poderão indicar o valor disponível para investimento na parceria e o compartilhamento de resultados provenientes da parceria, respeitando-se a participação mínima da PRODAM em 50%.

7. Do julgamento das propostas

A Comissão Especial designada pela Instrução Normativa 053/2025 (Documento SEI 147275030) julgará as propostas de parceria a partir dos seguintes critérios:

a) Potencial da solução e alinhamento estratégico com os objetivos da PRODAM-SP e da Administração Pública em geral, que poderá ser beneficiária da ferramenta: apurados a partir dos critérios de capacidade técnica;
b) Viabilidade e maturidade do modelo de negócio da solução proposta;
c) Modelo Financeiro, projeções de investimento e Estratégia Comercial.
d) Estimativa de receitas para a PRODAM-SP e para o Parceiro, incluindo a proposta de compartilhamento de resultados.
e) Estrutura de Governança da Parceria e Gestão de Riscos.

7.1. Da Comissão Especial

Foi designada uma Comissão Especial para a Seleção de Parceiro Privado, segundo a instrução IN-E 053/2025cujas funções e competências estão lá determinadas.

CRITÉRIOS DA POC - SMART SAMPA PRODAM				
Requisito Funcional Obrigatório	Descrição Detalhada do Caso de Teste	Método de Aferição	Descrição	Atende
Instalação das câmeras	Instalar e colocar em operação todas as câmeras previstas na POC, garantindo ingestão contínua de vídeo. Validar a integração estável com os hardwares (câmeras e sensores) de ao menos 2 fabricantes distintos, demonstrando compatibilidade física e lógica. Registrar evidências de operação por meio de logs de sistema.	Verificação física dos equipamentos instalados + exibição no sistema + logs de ingestão de vídeo por câmera. Apresentar registro de integração com no mínimo 2 fabricantes/modelos distintos de câmeras.	Compatibilidade com Dispositivos e Protocolos Diversos	
Visualização em tempo real	Exibir vídeo ao vivo com baixa latência. Demonstrar a visualização simultânea de múltiplas câmeras no dashboard. Registrar evidência objetiva da latência medida por meio de log de sistema ou ferramenta de medição.	Medição objetiva de latência (exibindo o tempo de latência): comparação cronometrada entre ação real e exibição na tela, com registro em log. Captura de evidência do timestamp do sistema no momento da ação e no momento da exibição. Resultado de exemplo: latência ≤ 2s.	Disponibilidade e Continuidade Operacional	
Gravação e reprodução de vídeo	Gravar continuamente o fluxo de vídeo de todas as câmeras da POC e demonstrar a capacidade de recuperar trechos específicos por câmera, período e evento. Evidenciar por meio de logs do sistema a integridade temporal das gravações (sem gaps) e o tempo de resposta para recuperação do trecho solicitado.	Solicitação de ao menos 3 trechos de vídeo com critérios distintos (câmera, horário, evento). Verificação de retorno correto + análise de logs de gravação confirmando continuidade temporal. Medir e registrar o tempo de recuperação de cada trecho.	Políticas de Retenção / Logs e Auditoria	
Multi-stream / Ajuste automático	Demonstrar o ajuste automático de qualidade de vídeo conforme condições de rede, mantendo a operação do sistema sem interrupção. Simular cenário de degradação de rede (perda de pacotes) e registrar em log o comportamento do sistema: resolução adotada, bitrate, alertas gerados e tempo de adaptação.	Simulação controlada de perda de pacotes. Para cada cenário: captura de logs do sistema mostrando a mudança automática de resolução/bitrate, tempo de adaptação e eventuais alertas. Resultado registrado em relatório de teste com evidências.	Escalabilidade / Compatibilidade com Protocolos	
Reconhecimento facial	Detectar rostos em vídeo ao vivo e identificar pessoas previamente cadastradas em base de dados. O sistema deve gerar alerta automático para os cadastrados e registrar log com score de confiança, timestamp e câmera de origem.	Passagem controlada de voluntários cadastrados e não cadastrados. Verificação de: (a) alertas automáticos gerados para cadastrados; (b) ausência de falsos positivos para não cadastrados; (c) logs com score de confiança ≥ limiar definido, timestamp e ID da câmera. Evidência via trilha de auditoria do sistema.	Análises Inteligentes por IA	
OCR / LPR de placas	Reconhecer placas de veículos em movimento (padrão Mercosul e antigo) com velocidade compatível ao cenário urbano (até 80 km/h). Demonstrar com ao menos 5 passagens reais ou simuladas em condições distintas (dia, noite, chuva se aplicável). O sistema deve registrar log com placa reconhecida, score de confiança, timestamp, câmera e imagem de evidência.	Passagens reais ou simuladas de veículos com placas conhecidas. Comparação entre placa real e placa reconhecida pelo sistema. Verificação de logs com: placa detectada, confiança, timestamp, câmera de origem e imagem capturada. Taxa de acerto mínima: ≥ 90% das passagens.	Análises Inteligentes por IA	

Detecção de comportamento suspeito	Identificar automaticamente ao menos 3 tipos de comportamento anômalo: corrida/movimentação brusca, queda de pessoa e objeto abandonado. Realizar simulações controladas para cada tipo (mínimo 2 tentativas por tipo). O sistema deve gerar alerta automático com classificação do evento, timestamp, câmera e imagem/clipe de evidência.	Simulações controladas para cada tipo de comportamento (mínimo 6 simulações no total). Para cada evento: verificar geração de alerta automático + log com classificação, timestamp, câmera e evidência visual. Registrar taxa de detecção e eventuais falsos positivos em relatório de teste.	Detecção Automática de Eventos
Contagem de pessoas e veículos	Contar o fluxo de pessoas e veículos em zonas específicas configuradas no sistema. O sistema deve apresentar contagem acumulada e log com cada detecção individual (timestamp, tipo, direção e zona).	Passagens controladas com quantidade conhecida. Comparação entre contagem real e contagem do sistema. Verificação de logs individuais de detecção. Taxa de acerto mínima: ≥ 85%. Evidência: relatório de contagem do sistema + logs detalhados.	Análises Inteligentes por IA
Busca forense por atributos	Buscar pessoas e veículos por características visuais (cor de roupa, tipo de veículo, cor do veículo, placa parcial, faixa horária).	Execução de 3 buscas com critérios diferentes diretamente no sistema. Verificação da relevância e precisão dos resultados. Evidência: logs da consulta (parâmetros buscados, quantidade de resultados, timestamp) e captura de tela dos resultados.	Recursos de Análise Forense
Linha do Tempo Forense	Reconstruir a sequência de eventos em ordem cronológica para um período e região selecionados, correlacionando alertas, detecções e gravações. Demonstrar a geração de timeline para ao menos 1 cenário completo de investigação, com eventos de diferentes tipos.	Seleção de período e região no sistema, geração da timeline e verificação da ordem cronológica e completude dos eventos. Evidência: exportação ou captura da timeline gerada + logs de consulta ao sistema.	Recursos de Análise Forense
Heatmap (Mapa de calor)	Gerar mapa de calor de eventos (movimentação, alertas, detecções) para áreas monitoradas pela POC. Demonstrar a geração para ao menos 2 tipos de eventos distintos e 2 períodos temporais diferentes.	Solicitação de relatório de mapa de calor no sistema. Verificação visual da representação + validação de coerência com os eventos registrados nos logs. Evidência: exportação do mapa de calor + logs de eventos correspondentes.	Recursos de Análise Forense
Dashboard operacional	Exibir dashboard com mapa georreferenciado das câmeras, status em tempo real (online/offline), alertas ativos, incidentes em andamento e KPIs operacionais (ex: total de alertas/dia, tempo médio de resposta). Demonstrar navegação funcional e atualização em tempo real dos indicadores.	Navegação completa pelo dashboard demonstrando cada componente funcional. Verificação da atualização em tempo real ao gerar um novo alerta durante o teste. Evidência: logs de atualização do dashboard + captura de tela dos componentes.	Suporte Multiplataforma / Interface Modular
Orquestração de incidentes (OMS)	Criar incidentes automaticamente a partir de alertas gerados pelo sistema (detecção de comportamento, reconhecimento facial, LPR). Demonstrar a criação automática de ao menos 3 incidentes a partir de alertas distintos, com classificação, prioridade e vinculação à evidência original (câmera, clipe, alerta).	Simulação de 3 eventos distintos que gerem alertas → verificação da criação automática de incidentes no OMS. Para cada incidente: verificar classificação, prioridade, evidência vinculada e log do sistema registrando toda a cadeia (alerta → incidente).	Gestão de Incidentes (OMS)

Despacho para agente	Enviar ocorrência do OMS ao dispositivo/sistema do agente de campo, com informações do incidente (localização, tipo, prioridade, evidência). Medir o tempo entre a criação do incidente e o recebimento pelo agente.	Criação de ocorrência no OMS e comprovação de envio de dados ao sistema destino via integração. Medição cronometrada do tempo de entrega. Evidência: log do sistema com timestamps de envio e confirmação de recebimento a partir de um sistema simulado + captura no dispositivo do agente. Será realizada simulação com consumo de API definida no momento da POC.	Suporte Multiplataforma / Integração OMS
Retorno do agente via sistema	Agente de campo envia dados de atendimento (status, fotos, observações) e realiza o fechamento da ocorrência diretamente pelo sistema/dispositivo móvel.	Teste em campo: agente atualiza status, anexa evidência e fecha ocorrência. Evidência: log do sistema com timestamps de envio e confirmação de recebimento a partir de um sistema simulado + captura no dispositivo do agente. Será realizada simulação com consumo de API definida no momento da POC.	Suporte Multiplataforma
Conectividade 4G/5G	Validar a capacidade de operação via rede móvel (4G/5G) nos ambientes definidos na POC, considerando variações normais de conectividade. Demonstrar que o sistema mantém operação funcional (visualização, alertas, gravação) mesmo em condições de rede móvel.	Registrar em log: momento da queda, momento da retomada via 4G/5G, funcionalidades mantidas e eventuais degradações. Evidência: logs do sistema + relatório de teste.	Disponibilidade e Continuidade Operacional
Fallback automático de rede	Demonstrar mecanismo de alternância automática entre links de comunicação (principal e secundário) com preservação da operação na central de monitoramento. O failover deve ocorrer sem intervenção manual e sem perda de dados críticos.	Desconectar link principal e medir: (a) tempo de detecção da falha; (b) tempo de comutação para link secundário; (c) continuidade das funcionalidades na central. Evidência: logs do sistema com timestamps de falha, comutação e restabelecimento + alertas automáticos gerados.	Disponibilidade e Continuidade Operacional
Controle de acesso	Demonstrar acessos distintos por perfis de usuário com permissões diferenciadas para visualização, operação e configuração.	Login com perfis distintos. Para cada perfil: verificar funcionalidades acessíveis e bloqueadas conforme a matriz de permissões. Evidência: logs de acesso (login, ações executadas, tentativas bloqueadas) para cada perfil testado.	Controle de Acesso
Segregação modular entre clientes	Demonstrar que usuários de clientes/órgãos diferentes não acessam dados cruzados (câmeras, gravações, alertas, incidentes de outro cliente). Testar com ao menos 2 perfis de clientes distintos.	Criação de perfis simulados de 2 clientes distintos. Tentativa de acesso cruzado a dados do outro cliente. Verificação de bloqueio total. Evidência: logs de tentativa de acesso negado + trilha de auditoria do sistema.	Controle de Acesso / Portabilidade e Migração / Arquitetura Modular
Segurança de comunicação (HTTPS)	Garantir que toda comunicação entre componentes do sistema (câmeras, servidores, dashboard, agentes) utiliza criptografia TLS/HTTPS.	Inspeção de certificados digitais em cada interface de comunicação. Verificação via ferramenta de rede (ex: Wireshark ou equivalente) da ausência de tráfego HTTP puro. Evidência: relatório de inspeção de certificados + captura de análise de tráfego.	Criptografia

Monitoramento de integridade	Detectar automaticamente câmera ou componente offline e gerar alerta ao operador em tempo real. Demonstrar com a desconexão controlada de ao menos 2 câmeras e 1 componente de infraestrutura.	Desconexão controlada de câmeras/componentes. Verificação de: (a) tempo para detecção da falha; (b) alerta gerado ao operador; (c) registro no dashboard. Evidência: logs com timestamp de desconexão, detecção e alerta + captura do dashboard.	Observabilidade e Telemetria
Observabilidade mínima (logs)	Registrar automaticamente todos os eventos relevantes do sistema: login/logout, alertas gerados, incidentes criados/fechados, ações de operador, falhas de componente.	Execução de ao menos 10 ações distintas no sistema e verificação da geração de logs correspondentes. Consulta aos logs para confirmar completude e formato. Evidência: exportação de logs + demonstração da interface de consulta.	Logs e Auditoria
Compatibilidade entre fabricantes distintos	Conectar e operar câmeras de ao menos 2 fabricantes distintos utilizando protocolos de interoperabilidade diversos.	Adição de câmera de fabricante diferente ao sistema durante o teste. Verificação de funcionamento completo (vídeo, alertas, gravação) da nova câmera. Evidência: logs de integração da câmera + demonstração funcional.	Compatibilidade com Dispositivos e Protocolos Diversos
Atualização não disruptiva	Demonstrar a capacidade de atualizar ou alterar módulo do sistema sem indisponibilidade crítica da operação. A atualização deve preservar gravações em andamento e alertas ativos.	Ativação/desativação de funcionalidade ou módulo durante operação. Verificação de: (a) continuidade da operação geral; (b) preservação de gravações; (c) manutenção de alertas. Evidência: logs do sistema antes, durante e após a atualização + relatório de impacto.	Versionamento e Atualizações Contínuas
Integração com API escolhida em momento da POC	Enviar eventos e alertas para endpoint escolhido no momento da POC representando sistema municipal.	Configuração de endpoint + envio de eventos pelo sistema. Verificação do recebimento, formato e conteúdo de cada evento. Evidência: logs de envio do sistema + logs de recebimento + payload de cada evento.	Suporte a APIs e Integrações
Importação de base de dados	Importar base de dados contendo rostos e placas veiculares (base definida no contexto da POC). Validar a disponibilidade e integridade dos dados importados para uso nas funcionalidades de reconhecimento.	Carga da base no sistema. Verificação de disponibilidade dos registros importados via consulta ao sistema. Validação de integridade (total importado vs. total da base). Evidência: log de importação + relatório de integridade.	Normalização e Padronização de Metadados
Abertura manual de ocorrência	Operador cria incidente manualmente no OMS, com classificação, prioridade, descrição e vinculação opcional a câmera/evidência. Demonstrar a criação de ao menos 2 ocorrências manuais com classificações distintas.	Criação manual de ocorrências no sistema pelo operador. Verificação de: campos obrigatórios, classificação, prioridade e rastreabilidade. Evidência: logs do sistema com registro de criação + dados da ocorrência.	Gestão de Incidentes (OMS)
Ajuste de regras e sensibilidade	Ajustar zonas de detecção, parâmetros de sensibilidade e regras dos mecanismos analíticos (ex: limiar de confiança do reconhecimento facial, zona de contagem, sensibilidade de detecção de comportamento). Demonstrar o impacto dos ajustes nas detecções.	Alteração de ao menos 3 parâmetros distintos com observação e registro do impacto nas detecções. Comparação antes/depois do ajuste. Evidência: logs de configuração (quem alterou, quando, valor anterior, valor novo) + logs de detecção mostrando a mudança de comportamento.	Capacidade de configurar zonas e parâmetros dos mecanismos analíticos, permitindo ajustes de sensibilidade e observação do impacto nas detecções.

Cenário end-to-end (fluxo operacional completo)	Executar fluxo completo de operação: detecção automática de evento → geração de alerta → criação de incidente no OMS → despacho para agente de campo → atendimento pelo agente → retorno de dados → fechamento da ocorrência. Demonstrar ao menos 2 cenários end-to-end com tipos de eventos distintos.	Simulação operacional completa de 2 cenários distintos. Para cada cenário: verificação de cada etapa do fluxo com logs e timestamps. Medição do tempo total do ciclo. Evidência: trilha de auditoria completa de cada cenário (logs de cada módulo envolvido) + relatório consolidado.	Demonstração do fluxo completo de operação, da detecção do evento até o encerramento da ocorrência, validando a integração entre os módulos da solução.
Disponibilidade operacional durante a POC	Avaliar a estabilidade da solução durante todo o período da POC em ambiente real. O sistema deve manter operação contínua, sendo toleradas apenas indisponibilidades breves e justificadas para testes controlados. Registrar todos os incidentes de indisponibilidade.	Monitoramento contínuo da operação durante a POC. Registro de todas as indisponibilidades com: timestamp de início/fim, causa raiz, módulos afetados e ação corretiva. Testes controlados de falha podem ser realizados em janelas programadas. Evidência: relatório de disponibilidade com logs do sistema + registro de incidentes.	Avaliação da estabilidade da solução durante a POC e da arquitetura proposta para atendimento a requisitos de disponibilidade de SLA em produção.
Contingência e recuperação de gravação	Demonstrar a capacidade de preservar ou recuperar gravações em caso de falha controlada do componente de armazenamento primário. O sistema deve evidenciar a estratégia de redundância (replicação, backup ou buffer local).	Simulação controlada de indisponibilidade do armazenamento primário. Verificação de: (a) continuidade ou recuperação das gravações; (b) tempo de recuperação; (c) integridade dos dados recuperados. Evidência: logs do sistema mostrando a falha, ativação do contingente e recuperação + verificação de integridade dos vídeos.	Demonstração da estratégia de redundância e contingência para armazenamento de dados em caso de falha do componente primário.
Integração com sistemas externos	Demonstrar a capacidade de integração bidirecional (APIs de entrada e saída) com sistemas e bases de dados definidos pela PRODAM ou disponibilizados no contexto da POC. Validar interoperabilidade, troca de eventos e compatibilidade técnica.	Execução de testes de integração com sistemas/bases disponibilizados na POC. Verificação de envio, recebimento e processamento de eventos em ambas as direções. Evidência: logs de integração + registros nos sistemas de destino + payloads trocados.	Demonstração da capacidade técnica de integração com sistemas municipais, preferencialmente por meio de ambientes simulados ou controlados na POC.
Base de veículos furtados/fugitivos	Consultar e correlacionar eventos de LPR com bases de dados de veículos (real ou simulada, definida pela PRODAM). Demonstrar alerta automático ao detectar placa presente na base de busca.	Passagem de veículo com placa cadastrada na base de busca. Verificação de: (a) alerta automático gerado; (b) correlação correta com o registro da base; (c) tempo de resposta. Evidência: logs do sistema com detecção, correlação e alerta + registro da consulta à base.	Demonstração de compatibilidade técnica para consulta e correlação com bases de dados estruturadas..
SLA de Suporte Técnico / Field Service	Apresentar modelo de suporte técnico proposto com definição de níveis de atendimento (Ex.: N1, N2, N3), tempos de resposta por severidade e estrutura de equipe. Demonstrar capacidade de registro e acompanhamento de chamados durante a POC.	Demonstração do sistema de chamados (abertura, classificação, acompanhamento). Medição de tempo de resposta para ao menos 1 chamado simulado. Evidência: documentação do modelo + logs do sistema de chamados.	Apresentação do modelo de suporte técnico proposto, incluindo níveis de atendimento e tempos de resposta.

Relatórios gerenciais mensais (O título pode ser mudado, talez pedir um exemplo de relatório do sistema ou exportação de dado para tal finalidade)	Gerar relatórios consolidados a partir dos dados produzidos durante a POC, demonstrando a capacidade do operador de selecionar e configurar os dados exibidos, incluindo: período temporal, tipos de evento, câmeras/regiões, incidentes, indicadores de disponibilidade, métricas operacionais e KPIs. O sistema deve permitir que o usuário escolha quais informações compõem o relatório conforme sua necessidade. Demonstrar capacidade de exportação dos dados e relatórios para análise externa.	Geração de ao menos 2 relatórios distintos (operacional e gerencial), demonstrando a seleção de filtros e indicadores pelo operador. Verificação de que o usuário consegue personalizar o conteúdo do relatório (selecionar período, tipo de evento, região, KPIs). Demonstração de exportação em formato aberto (CSV, PDF ou equivalente). Evidência: relatórios gerados com configurações distintas + logs de exportação.	Capacidade de geração de relatórios consolidados com indicadores de disponibilidade, ocorrências e eventos relevantes.

ANEXO III – Requisitos da Proposta

1. PROPOSTA

1.1 As INTERESSADAS deverão encaminhar proposta contendo:

1.1.1 Informações gerais sobre a empresa;

1.1.2 Detalhamento funcional da solução proposta;

1.1.3 Declaração expressa da indicação de disponibilidade para, em conjunto com a PRODAM e por prazo determinado, arcar com os respectivos custos decorrentes de eventuais estratégias comerciais para alavancagem de vendas, tais como: demonstrações, provas de conceito, experimentações e/ou degustações da solução a potenciais clientes.

1.1.4 Demais informações que sirvam de insumo para a análise, pela PRODAM, da capacidade de qualificação técnica para a celebração de futura parceria de negócio.

1.1.5 É permitido às INTERESSADAS apresentarem soluções que explorem todos os matizes e variáveis que aos seus juízos possam influenciar o retorno econômico da oportunidade de negócio.

2. QUALIFICAÇÃO TÉCNICA

2.1 A qualificação técnica visa comprovar que a INTERESSADA possui capacidade preexistente, ou seja, com base em sua experiência anterior ao presente edital.

2.2 Requisitos funcionais: as INTERESSADAS deverão encaminhar evidências que demonstrem que a solução proposta atende aos requisitos listados no ANEXO IV - PLANILHA DE QUALIFICAÇÃO TÉCNICA - REQUISITOS FUNCIONAIS.

2.3 Requisitos de capacidade: as INTERESSADAS deverão encaminhar evidências que demonstrem o atendimento aos requisitos listados no ANEXO V - PLANILHA DE QUALIFICAÇÃO TÉCNICA - REQUISITOS DE CAPACIDADE.

2.3.1 Os atestados de capacidade técnica devem se referir à implementação de solução igual ou semelhante ao objeto do presente edital;

2.3.2 Os atestados de capacidade técnica devem conter local, data e assinatura do emissor, o número ou identificação do contrato, o escopo do projeto, o cronograma de implantação e os resultados alcançados;

2.3.3 Os atestados de capacidade técnica devem ser emitidos em nome do(a) tomador(a) do serviço, por ente público ou empresa privada, nacional ou estrangeira.

2.4 Requisitos de Sustentabilidade: as INTERESSADAS devem encaminhar evidências que demonstrem o atendimento aos requisitos listados no ANEXO V - PLANILHA DE QUALIFICAÇÃO TÉCNICA - REQUISITOS DE CAPACIDADE .

2.5 As INTERESSADAS deverão encaminhar as planilhas do ANEXO IV e do ANEXO V em formato/extensão ".PDF" e ".xlsx", devidamente preenchidas com a alimentação apenas das colunas “Atende?”, “Evidência*” e “QTD” relacionada a “Autodeclaração da INTERESSADA”

3. CLASSIFICAÇÃO

3.1 A classificação técnica das propostas será realizada com base na soma da pontuação dos requisitos atendidos:

Qualificação Técnica	Pontos
Requisitos Funcionais	Nota x 40%
Requisitos de Capacidade	Nota x 60%
Total	

EDITAL DE CHAMAMENTO PÚBLICO PARA SELEÇÃO DE PARCEIRO PRIVADO

Item	Titulo	Descrição dos requisitos de qualificação técnica	Motivação/Finalidade	Forma de Demonstração	Critério de Aceitação	Pontos	Tipo
1	Arquitetura modular	A solução deve adotar arquitetura modular, permitindo que componentes como ingestão de vídeo, analytics, armazenamento, despacho e visualização funcionem de forma independente, facilitando manutenção, evolução e integração futura.	Garantir flexibilidade tecnológica, possibilitar atualizações em módulos específicos sem afetar todo o sistema e permitir expansão gradual conforme a necessidade do município.	documentação técnica, diagrama de arquitetura, manual da solução, declaração do fabricante	Apresentação de documentação que comprove que a solução é composta por módulos independentes e interoperáveis.	10	Arquitetura e Infraestrutura
2	Escalabilidade	A solução deve suportar expansão progressiva do número de dispositivos, usuários e volume de dados, permitindo aumento da capacidade operacional sem necessidade de reestruturação completa da plataforma, desde que tecnicamente justificável.	Garantir que a plataforma acompanhe o crescimento do município e a evolução do parque tecnológico, mantendo desempenho adequado mesmo em cenários de maior carga e complexidade.	Documentação técnica, estudos de capacidade, histórico de operação em ambientes ampliados, declaração do fabricante	Apresentação de documentação que comprove que a solução suporta expansão gradual de dispositivos, usuários e dados, de forma coerente e tecnicamente sustentada.	10	Arquitetura e Infraestrutura
3	Políticas de retenção	A solução deve permitir configuração de diferentes prazos de retenção de dados, variando de acordo com o tipo de evento, câmera ou necessidade operacional. (ex: retenção ampliada para eventos marcados, conforme diretrizes legais).	Atender normas legais, auditorias e demandas específicas de segurança pública, permitindo gestão adequada do armazenamento.	Documentação técnica, manual da solução, prints ilustrativos, declaração do fabricante	Comprovação documental de que a plataforma oferece políticas configuráveis de retenção por categoria de dados.	7	Dados e Armazenamento
4	SaaS operacional	A solução deve ser disponibilizada no modelo SaaS, com gestão de atualizações, monitoramento, segurança e operação sob responsabilidade da contratada. A plataforma deve permitir implantação e execução em ambiente de hospedagem definido pela Administração Pública, incluindo o datacenter da PRODAM, desde que atendidos os requisitos técnicos da solução e sem dependência exclusiva de infraestrutura proprietária externa.	Garantir operação contínua, manutenção centralizada e menor esforço operacional para a Administração, preservando a capacidade de hospedar a solução em ambiente próprio por razões de segurança, governança de dados e políticas institucionais.	Documentação técnica, arquitetura da solução, indicação de ambientes SaaS já operados, declaração do fabricante	Apresentação de documentação que comprove o modelo SaaS da solução e a possibilidade de sua execução em ambiente de hospedagem indicado pela Administração, incluindo datacenter próprio.	10	Arquitetura e Infraestrutura
5	Criptografia	A solução deve utilizar criptografia para proteger dados em trânsito e em repouso, adotando protocolos amplamente aceitos, como HTTPS e padrões equivalentes.	Garantir segurança dos dados e conformidade com boas práticas.	Documento técnico, declaração do fabricante, política de segurança, whitepaper	Comprovação documental do uso de criptografia para dados em trânsito e em repouso, sem exigência de algoritmos específicos.	8	Segurança e Controle de Acesso
6	LGPD e Compliance	A solução deve comprovar aderência aos princípios da LGPD, incluindo anonimização de dados, registro de operações, proteção de dados pessoais e mecanismos de privacidade incorporados ao design.	Garantir conformidade legal, reduzir riscos jurídicos e assegurar governança de proteção de dados.	Declaração de conformidade, política de privacidade, documentação de Privacy by Design, relatório de governança	Apresentação de documentação que comprove a adoção de práticas alinhadas aos princípios da LGPD.	5	Compliance e Governança
7	Plano de escalabilidade	A solução deve apresentar plano técnico de expansão que contemple crescimento de dispositivos, usuários, tráfego, armazenamento e processamento, demonstrando compatibilidade com operações de larga escala.	Garantir que a plataforma possa evoluir acompanhando a expansão territorial e operacional do município.	Documento técnico, estimativa de sizing, modelo de capacidade, histórico de uso em outros clientes	Plano detalhado, coerente e tecnicamente viável, demonstrando previsibilidade de expansão. Prever o cenário de ociosidade, considerando a diminuição de ambiente.	10	Arquitetura e Infraestrutura
8	Logs e Auditoria	A solução deve registrar eventos relevantes de operação, acesso, falhas, alterações de configuração e ações executadas pelos usuários, mantendo trilha de auditoria completa e rastreável. Os registros devem permitir identificar responsáveis, horários, ações realizadas e contexto do evento.	Garantir rastreabilidade, segurança operacional, transparência no uso da plataforma e suporte à investigação de incidentes técnicos ou de segurança	Documentação técnica, política de auditoria, descrição dos tipos de logs gerados, arquitetura de registro de eventos, e plano de temporalidade dos registros.	Apresentação de documentação que comprove que a solução mantém registros de auditoria abrangentes, com identificação de ações, usuários, timestamps e eventos relevantes para acompanhamento operacional e segurança. Devendo registrar a não exclusão de registros de logs.	8	Segurança e Controle de Acesso
9	Controle de Acesso e Identidade	A solução deve permitir o gerenciamento de diferentes níveis de acesso por meio de perfis, papéis ou grupos de usuários, garantindo que cada usuário visualize e execute apenas as funcionalidades compatíveis com suas atribuições. O sistema deve possibilitar configuração granular das permissões e registro das ações autorizadas, bem como ativar e desativar acessos.	Assegurar que o uso da plataforma atenda aos princípios de segregação de funções, governança e segurança da informação, evitando acessos indevidos a dados ou funcionalidades sensíveis.	Documentação técnica, manual de administração, exemplos de perfis e permissões, declaração do fabricante.	Comprovação documental da existência de perfis e controles de acesso robustos.	8	Segurança e Controle de Acesso
10	Disponibilidade e Continuidade Operacional	A solução deve possuir arquitetura que suporte operações contínuas, permitindo a aplicação de atualizações sem interrupção total do serviço.	Garantir operação 24x7 de serviços essenciais de segurança pública, assegurando que manutenções de rotina não comprometam o funcionamento da plataforma.	Documento técnico, política de atualização, declaração do fabricante, descrição do processo de release.	Comprovação documental de que a solução suporta atualizações com impacto reduzido, sem exigir interrupção total da plataforma.	6	Operação e Monitoramento
11	Suporte a APIs e Integrações Padronizadas	A plataforma deve disponibilizar APIs documentadas (preferencialmente RESTful) ou mecanismos equivalentes que permitam integração bidirecional com sistemas legados e de terceiros, incluindo sistemas de segurança pública, CET, PM, Bombeiros, Defesa Civil e órgãos municipais. As APIs devem seguir padrões de mercado com documentação técnica acessível, versionamento e controle de autenticação. Deve suportar tanto o envio quanto o recebimento de dados e eventos.	A plataforma deve disponibilizar APIs documentadas (preferencialmente RESTful) ou mecanismos equivalentes que permitam integração bidirecional com sistemas legados e de terceiros, incluindo sistemas de segurança pública, CET, PM, Bombeiros, Defesa Civil e órgãos municipais. As APIs devem seguir padrões de mercado com documentação técnica acessível, versionamento e controle de autenticação. Deve suportar tanto o envio quanto o recebimento de dados e eventos.	Documentação de API com exemplos de endpoints, payloads e autenticação. Guia de integração descrevendo cenários de uso com sistemas externos. Declaração do fabricante.	Apresentação de documentação oficial demonstrando suporte a APIs bidirecionais com versionamento, autenticação e documentação técnica acessível para integradores.	7	Integração e Interoperabilidade
12	Normalização e Padronização de Metadados	A solução deve ser capaz de padronizar informações vindas de diferentes tipos de câmeras e sensores, permitindo que o sistema entenda tudo de forma organizada e uniforme.	Permitir que diferentes câmeras e sensores gerem eventos padronizados para visualização, análise e despacho.	Documento técnico, guia de metadados, descrição da arquitetura.	Comprovação documental de que a plataforma padroniza dados provenientes de múltiplas fontes.	7	Integração e Interoperabilidade
13	Versionamento e Atualizações Contínuas	A solução deve possuir política clara de versionamento e gerenciamento de atualizações, incluindo registro das versões liberadas, descrição das melhorias implementadas e procedimentos para atualização controlada da plataforma. As atualizações devem seguir processo estruturado, permitindo planejamento e acompanhamento pela Administração.	Assegurar rastreabilidade da evolução da plataforma, transparência das alterações realizadas e previsibilidade no planejamento das atualizações, sem prejuízo das operações do município.	Documentação técnica, política de versionamento, exemplos de changelog, declaração do fabricante	Apresentação de documentação que comprove a existência de política formal de versionamento e processo estruturado de atualização, incluindo registro de versões e melhorias, listando item a item da atualização.	5	Compliance e Governança
14	Suporte Multiplataforma	A solução deve permitir acesso via navegadores modernos e, quando aplicável, aplicativos móveis para uso em campo.	Permitir operação tática e mobilidade para agentes públicos.	Documento técnico, manual do sistema, declaração do fabricante	Comprovação documental de que a solução opera em múltiplas plataformas. Relatório de testes em cada navegador testado.	4	Usabilidade e Interface
15	Observabilidade e Telemetria	A solução deve oferecer métricas, monitoramento e indicadores sobre desempenho, carga, falhas e utilização.	Garantir transparência operacional e capacidade de diagnóstico.	Documento técnico, manual, prints exemplificativos, declaração do fabricante	Comprovação documental da existência de recursos de monitoramento e telemetria.	6	Operação e Monitoramento
16	Monitoramento de Integridade dos Dispositivos	A solução deve permitir a monitoração do status de câmeras, sensores, gateways e demais equipamentos conectados.	Garantir visualização de falhas, quedas e necessidades de manutenção.	Documento técnico, guia de dispositivos, declaração do fabricante	Comprovação documental da capacidade de monitoramento de integridade. Painel administrativo que permita a visualização no mapa dos dispositivos e seus status, e que o painel possua filtros para facilitação de navegação e identificação dos dispositivos.	6	Operação e Monitoramento
17	Compatibilidade com Dispositivos e Protocolos Diversos	A solução deve suportar câmeras e dispositivos heterogêneos utilizando padrões amplamente aceitos no mercado.	Facilitar a integração com o parque já existente e evitar dependência tecnológica.	Documento técnico, lista de compatibilidade, declaração do fabricante	Comprovação documental de suporte a dispositivos variados e protocolos padrão. Lista de tipos de dispositivos previamente homologados (modelos ou características)	7	Integração e Interoperabilidade
18	Suporte a Múltiplos Protocolos de Comunicação	A solução deve operar com diferentes meios e protocolos de comunicação (ex.: fibra, LTE/4G/5G, Wi-Fi Mesh, IoT, rádio).	Garantir interoperabilidade em diferentes cenários urbanos.	Documento técnico, declaração do fabricante	Documentação que confirme suporte a múltiplos protocolos.	7	Integração e Interoperabilidade
19	Conformidade com Normas de Segurança Urbana e TIC	A solução deve observar normas, boas práticas e diretrizes amplamente reconhecidas no setor de tecnologia da informação e segurança urbana, garantindo que seus componentes, processos e integrações sigam padrões adotados pelo mercado e compatíveis com políticas institucionais da Administração Pública.	Assegurar que a plataforma opere em conformidade com práticas consolidadas de segurança, governança e qualidade, reduzindo riscos operacionais e garantindo integração segura com o ecossistema municipal.	Documentação técnica, políticas internas de segurança da solução, declaração do fabricante confirmando aderência a práticas reconhecidas	Comprovação documental de que a solução adota práticas amplamente aceitas de segurança e tecnologia da informação, condizentes com padrões utilizados pelo setor público e compatíveis com as diretrizes institucionais da Administração.	5	Compliance e Governança
20	Auditoria Avançada de Eventos e Ações	A solução deve registrar ações críticas de usuários e eventos relevantes para fins de rastreabilidade.	Apoiar investigações, controles e conformidade institucional.	Documento técnico, prints de auditoria, declaração do fabricante	Comprovação documental da existência de trilhas de auditoria. Garantia de não exclusão de trilha de auditoria.	8	Segurança e Controle de Acesso

21	Gestão de Incidentes (OMS)	A solução deve possuir mecanismos que permitam registrar, classificar, encaminhar e acompanhar incidentes gerados pelas câmeras, sensores ou operadores, por meio de um sistema de orquestração e gerenciamento (OMS). Esse sistema deve possibilitar o fluxo estruturado de tratamento de eventos, garantindo que cada ocorrência receba encaminhamento adequado dentro do processo operacional definido pelo município.	Garantir fluxo operacional para centros integrados de comando.	Documento técnico, guia de operação, declaração do fabricante	Comprovação documental do modelo de gerenciamento de incidentes com fluxo rastreável, vinculação a evidências e medição de SLA.	8	Gestão de Incidentes e Fluxo Operacional
22	Mecanismos de Redundância de Dados	A solução deve possuir mecanismos de redundância para garantir a continuidade e a integridade das informações em caso de falhas de componentes. Deve documentar a estratégia de replicação adotada (síncrona/assíncrona, local/remota).	Garantir continuidade e integridade dos dados em caso de falhas, com previsibilidade nos tempos de recuperação.	Documentação técnica com descrição da arquitetura de redundância, declaração do fabricante.	Comprovação documental de que a solução dispõe de mecanismos de redundância, documentados e fluxo rastreável de recuperação.	7	Dados e Armazenamento
23	Documentação Técnica e Manuais	O fornecedor deve apresentar documentação técnica mínima contendo especificações, arquitetura e guias de uso.	Garantir clareza, governança e capacidade de auditoria futura.	Documentação completa, manuais, guias de usuário	Entrega de documentação mínima exigida, conforme descrição	5	Compliance e Governança
24	Administração Centralizada	A solução deve disponibilizar mecanismos, padrões e interfaces que permitam, presente ou futuramente, a unificação operacional em um painel administrativo central — incluindo gestão de dispositivos, usuários, eventos, integrações e configurações.	Facilitar gestão operacional pelo município.	Documento técnico da arquitetura, manuais de administração, descrição de APIs e mecanismos de integração, declaração formal do fabricante sobre capacidade de unificação administrativa.	Comprovação documental de que a solução possui arquitetura, APIs e módulos que permitem centralizar, integrar ou federar informações em um console administrativo único, ainda que não completamente implementado na fase de POC.	6	Operação e Monitoramento
25	Portabilidade e Migração de Dados	A solução deve permitir a extração completa e estruturada de todos os dados, incluindo vídeos, metadados, ocorrências, logs, cadastros, integrações e demais informações operacionais, de forma a possibilitar a migração para outra plataforma no término do contrato. A contratada deve apresentar plano de migração com formatos abertos ou documentados para garantir a portabilidade.	Evitar dependência tecnológica ("lock-in"), assegurar a continuidade do serviço público ao final do contrato e garantir que o município mantenha a posse e o pleno uso de seus dados históricos.	Declaração do fabricante, documentação técnica de exportação, plano de migração, descrição dos formatos de dados	Comprovação documental de que a solução permite exportação completa de dados em formatos abertos ou documentados, com plano de migração apresentado.	7	Dados e Armazenamento
26	Plano de Continuidade Operacional e Recuperação de Desastres (Disaster Recovery)	A contratada deve apresentar plano formal de continuidade de negócios e recuperação de desastres, contendo procedimentos, prazos e níveis de serviço para restabelecimento da plataforma em situações de falha grave, indisponibilidade, corrupção de dados ou desastre natural.	Assegurar a disponibilidade da plataforma em cenários críticos, preservando a integridade de dados e garantindo a retomada rápida dos serviços essenciais de segurança urbana.	Plano de continuidade, política de disaster recovery, documento técnico, declaração do fabricante	Plano apresentado deve conter estratégias claras de recuperação, procedimentos operacionais e prazos compatíveis com o nível de criticidade da plataforma.	7	Dados e Armazenamento
27	Requisitos mínimos de segurança do acesso	A solução deve adotar mecanismos mínimos de segurança para autenticação e acesso, incluindo senha forte, proteção contra tentativas indevidas de login e conexão segura entre usuários e plataforma.	Garantir acesso seguro ao sistema, reduzindo riscos de uso indevido e protegendo informações sensíveis.	Documentação técnica, manual de autenticação, prints exemplificativos, declaração do fabricante	Comprovação documental de que a solução implementa mecanismos mínimos de segurança no acesso. Apresentação de certificados que possuirem.	8	Segurança e Controle de Acesso
28	Idioma da interface	A interface da solução deve disponibilizar o idioma português do Brasil ou permitir configuração para esse idioma.	Facilitar o uso pela equipe pública, garantindo compreensão adequada da solução.	Prints da interface, manual do usuário, documentação técnica, declaração do fabricante	Comprovação da existência de interface em português do Brasil ou de configuração equivalente.	4	Usabilidade e Interface
29	Personalização de identidade visual	A solução deve permitir personalização básica da identidade visual, incluindo logotipo da Administração Pública e ajustes simples na apresentação.	Alinhar a plataforma ao padrão institucional do município e facilitar identificação pelos usuários.	Prints ilustrativos, documentação técnica, manual de personalização, declaração do fabricante	Comprovação de que a solução permite ajustes básicos de identidade visual.	4	Usabilidade e Interface
30	Independência de ambiente de hospedagem	A solução deve ser capaz de operar em diferentes ambientes de hospedagem compatíveis, sem depender exclusivamente de infraestrutura proprietária do fornecedor. A plataforma deve permitir sua implantação em ambiente indicado pela Administração Pública, incluindo obrigatoriamente a possibilidade de execução no datacenter da PRODAM, desde que atendidos os requisitos técnicos previstos pela solução.	Garantir flexibilidade de implantação, evitar dependência de provedores específicos e assegurar que a Administração mantenha soberania sobre os ambientes de execução, conforme diretrizes de segurança, governança de dados e políticas institucionais	Documentação técnica, requisitos de infraestrutura, arquitetura da solução, declaração do fabricante. Declaração explícita de componentes da aplicação e de serviços consumidos externamentes se for o caso.	Apresentação de documentação que comprove que a solução pode ser implantada e operada em ambiente definido pela Administração Pública, incluindo datacenter próprio, sem necessidade de infraestrutura exclusiva do fornecedor.	10	Arquitetura e Infraestrutura
31	Análises inteligentes por IA (analytics)	A solução deve possuir mecanismos de análise inteligente baseados em algoritmos de visão computacional ou modelos de inteligência artificial, capazes de extrair metadados relevantes a partir das imagens, identificar padrões operacionais, detectar eventos de interesse e apoiar a atuação dos operadores. As capacidades devem incluir processamento automático para classificação, identificação de comportamentos e interpretação contextual das cenas monitoradas.	Reduzir dependência da observação manual, melhorar o tempo de resposta operacional, aumentar a precisão na identificação de situações críticas e aprimorar o uso dos recursos do município por meio de automação inteligente.	Documentação técnica, lista de funcionalidades analíticas suportadas, arquitetura de processamento, declaração do fabricante	Comprovação documental de que a solução disponibiliza mecanismos de análise inteligente para extração de metadados e identificação automática de eventos relevantes.	9	Inteligência Artificial e Analytics
32	Recursos de análise forense e reconstrução de eventos	A plataforma deve oferecer recursos para investigação e busca avançada em vídeos e eventos, permitindo consultas filtradas por atributos, reconstrução temporal de ocorrências, navegação por metadados e análise acelerada de grandes volumes de gravações. A solução deve apoiar a localização rápida de evidências e facilitar a compreensão de sequências de eventos.	Aprimorar a capacidade de investigação, reduzir o tempo de análise de gravações e possibilitar que operadores e órgãos de segurança identifiquem evidências de forma mais eficiente e segura.	Documentação técnica, descrição dos recursos de busca e reconstrução, exemplos de telas, declaração do fabricante	Comprovação documental de que a solução fornece ferramentas de análise forense com recursos avançados de busca, filtragem e reconstrução de eventos.	9	Inteligência Artificial e Analytics
33	Detecção automática de eventos	A solução deve permitir identificação automática de situações de interesse operacional, como eventos atípicos, comportamentos anormais ou ocorrências relevantes para segurança pública, mobilidade ou fiscalização urbana. Os eventos detectados devem ser convertidos em alertas estruturados e integrados ao fluxo de gestão de incidentes da plataforma.	Permitir resposta mais rápida a situações críticas, reduzir perda de eventos importantes, apoiar a tomada de decisão e aumentar a eficiência na operação do monitoramento urbano.	Documentação técnica, descrição dos tipos de eventos detectáveis, integração com o módulo de incidentes, declaração do fabricante	Comprovação documental de que a solução identifica automaticamente eventos relevantes e os integra ao fluxo de tratamento de incidentes.	9	Inteligência Artificial e Analytics
34	Extração e Padronização de Metadados de Vídeo	A solução deve fornecer mecanismos automáticos para extração, estruturação e padronização de metadados provenientes de vídeos, sensores e eventos, permitindo interoperabilidade entre subsistemas (VMS, IA, OMS e integrações externas) por meio de formatos documentados e consistentes.	Garantir uniformidade na interpretação de dados, facilitar buscas inteligentes, possibilitar integração com terceiros e viabilizar automações do OMS com base em informações estruturadas.	Documentação técnica, manual de metadados, diagrama de arquitetura, declaração do fabricante	Comprovação documental de que a solução possui mecanismo nativo de extração e padronização de metadados.	9	Inteligência Artificial e Analytics
35	Processamento Híbrido – Edge e Núcleo	A plataforma deve suportar arquiteturas híbridas que permitam processamento local em dispositivos de borda (edge) — quando disponível — e processamento no núcleo da plataforma, garantindo que funcionalidades críticas possam operar mesmo em condições de conectividade limitada.	Aprimorar desempenho, reduzir latência, aumentar resiliência e aproveitar recursos computacionais de câmeras inteligentes e gateways IoT.	Documentação técnica, descrição de topologias suportadas, declaração do fabricante	Demonstração documental de que a solução suporta arquiteturas híbridas edge + núcleo, com definição clara dos tipos de processamento realizados em cada camada.	10	Arquitetura e Infraestrutura
36	Integração Funcional entre VMS, IA e OMS	A solução deve garantir interoperabilidade entre os módulos de gestão de vídeo (VMS), análise inteligente (IA/analytics) e gestão de incidentes (OMS), permitindo que eventos detectados sejam automaticamente encaminhados ao fluxo de incidentes e vinculados às gravações e metadados correspondentes.	Assegurar que toda a operação ocorra de forma integrada, eliminando silos, aumentando eficiência operacional e garantindo rastreabilidade completa dos eventos.	Documentação técnica, arquitetura de integração, especificações de APIs internas, declaração do fabricante	Prova documental da existência de mecanismos nativos de integração entre VMS, IA e OMS, com fluxo automatizado de eventos.	7	Integração e Interoperabilidade
37	Funcionalidades Avançadas de Visualização Operacional	A plataforma deve oferecer mecanismos de visualização georreferenciada, dashboards operacionais, mapas de calor de eventos e sobreposição de informações provenientes de análises inteligentes, integrando elementos de sensores, câmeras e incidentes em uma interface unificada.	Apoiar a tomada de decisão em tempo real, aumentar situational awareness e permitir operação centralizada e eficiente da cidade.	Documentação técnica, prints ilustrativos, arquitetura de front-end, declaração do fabricante	Comprovação documental de que a plataforma oferece visualização georreferenciada e dashboards operacionais integrados ao fluxo de incidentes e aos metadados.	8	Gestão de Incidentes e Fluxo Operacional
38	Suporte a Sensores Inteligentes e Sinais Multimodais	A solução deve suportar ingestão, correlação e tratamento de dados multimodais oriundos de sensores inteligentes (presença, ruído, emergência, IoT), vinculando esses eventos às câmeras e ao OMS para geração de alertas ou investigação posterior.	Garantir que a plataforma seja multissensorial, expandindo a capacidade de monitoramento além do vídeo e oferecendo inteligência contextualizada.	Documentação técnica, especificações de protocolos suportados, declaração do fabricante	Demonstração documental de suporte a ingestão e correlação de dados de múltiplos sensores integrados ao fluxo de incidentes.	7	Integração e Interoperabilidade
39	Análise Acústica e Interpretação de Ruído	A plataforma deve suportar mecanismos de detecção e classificação de eventos acústicos (ex.: disparos, explosões, colisões, gritos), gerando metadados e integrando-os ao OMS como eventos passíveis de tratamento.	Aprimorar a capacidade do sistema de identificar situações críticas sem dependência exclusiva do vídeo, aumentando a abrangência do monitoramento.	Documentação técnica, lista de eventos acústicos reconhecidos, declaração do fabricante	Comprovação documental de que a solução realiza detecção e classificação de ruídos por mecanismos inteligentes.	9	Inteligência Artificial e Analytics
40	Fluxo Operacional Configurável no OMS	O módulo OMS deve permitir criação, edição e parametrização de fluxos de incidentes, incluindo regras de escalonamento, níveis de gravidade, diretrizes de despacho e integrações automatizadas com órgãos externos.	Adequar o OMS às diferentes realidades operacionais do município e evoluir continuamente o processo de gestão de incidentes.	Documentação técnica, descrição de workflows configuráveis, declaração do fabricante	Comprovação documental da capacidade de criação de fluxos customizáveis no OMS.	8	Gestão de Incidentes e Fluxo Operacional
41	Sincronização de Multi-stream e Gerenciamento Avançado de Vídeo	A solução deve suportar fluxo simultâneo de múltiplas resoluções (alta e baixa), marcação de eventos, sincronização temporal entre câmeras e recursos avançados de gerenciamento de vídeo, incluindo suporte a PTZ quando disponível.	Aprimorar desempenho, reduzir uso de banda, e garantir que o operador tenha acesso otimizado a vídeos ao vivo e gravados.	Documentação técnica, arquitetura VMS, declaração do fabricante	Prova documental de funcionalidades avançadas de gerenciamento de vídeo em conformidade com os padrões do mercado.	8	Gestão de Incidentes e Fluxo Operacional

42	Integridade e Cadeia de Custódia de Evidências	A solução deve oferecer mecanismos de preservação de integridade de evidências, incluindo hashing, watermarking ou recursos equivalentes, garantindo rastreabilidade e autenticidade das gravações exportadas.	Atender padrões legais de uso de imagens como evidência, assegurar confiabilidade e impedir adulteração de arquivos.	Documentação técnica, manual de exportação segura, declaração do fabricante	Comprovação documental de mecanismos de integridade e rastreabilidade de arquivos exportados.	8	Segurança e Controle de Acesso
43	Governança de Modelos de Inteligência Artificial	A plataforma deve dispor de mecanismos que permitam atualização, substituição, calibração e versionamento de modelos de IA utilizados para análises, garantindo evolutividade e conformidade contínua com o ambiente urbano.	Permitir evolução da solução, melhoria contínua e adaptação a novos cenários operacionais.	Documentação técnica, política de atualização de modelos, declaração do fabricante	Comprovação documental de governança de modelos de IA, incluindo processos de versionamento e substituição.	9	Inteligência Artificial e Analytics
44	Orquestração de Fluxo de Dados	A solução deve permitir a integração contínua e automática entre as camadas de captura, processamento (Edge), VMS, analytics, OMS e dashboards, garantindo fluxo consistente dos dados, metadados, alertas e eventos em toda a cadeia operacional.	Assegurar que toda a jornada do evento — da captura até o despacho — funcione sem rupturas, evitando sistemas desconectados, perda de dados, falhas na visualização e inconsistências operacionais.	Arquitetura técnica detalhada, documentação de APIs, fluxograma de orquestração, descrição de interoperabilidade entre VMS, IA e OMS	Comprovação documental de que a solução suporta trocas de dados entre as camadas conforme o fluxo operacional, demonstrando ingestão, processamento, geração de eventos e escalonamento integrado.	8	Gestão de Incidentes e Fluxo Operacional
45	Controle de Acesso por Domínio Operacional	A solução deve permitir definir permissões de visualização e operação com base em domínios como: território (bairros/zonas), grupos de câmeras, tipos de eventos, fluxos de despacho, relatórios e módulos específicos, garantindo que diferentes perfis tenham acesso apenas às informações compatíveis com sua função.	Garantir que, mesmo com múltiplos parceiros ou componentes durante a POC, a solução permita evolução para um ambiente integrado e administrável de forma centralizada, evitando fragmentação de sistemas e garantindo governança municipal a longo prazo.	Manual de perfis e permissões, documentação do sistema de gerenciamento de acesso, exemplos de configuração de permissões por perfil, território e tipo de evento	Comprovação documental de que a solução permite definir e aplicar regras de acesso segmentadas por função, território, grupo de ativos e tipo de evento.	8	Segurança e Controle de Acesso
46	Isolamento Modular e Segmentação Lógica de Dados Entre Clientes	A solução deve permitir o isolamento modular e a segmentação lógica de dados entre diferentes clientes da plataforma, garantindo que bases de dados, usuários, câmeras, incidentes e informações operacionais sejam separados conforme políticas de segurança e privacidade definidas pela PRODAM, enquanto módulos de aplicação, dashboards e componentes compartilhados possam ser reutilizados sem risco de acesso indevido.	Assegurar privacidade e segurança institucional entre diferentes clientes da solução (municípios, órgãos ou entidades contratantes), mantendo custos operacionais reduzidos e alta escalabilidade ao permitir compartilhamento de camadas de aplicação, preservando ao mesmo tempo o isolamento dos dados sensíveis de cada cliente.	Documentação da arquitetura de segmentação lógica, descrição das camadas que podem ser compartilhadas e das que são isoladas, declaração formal do fabricante, exemplos de políticas de isolamento modular	Comprovação documental de que a plataforma permite compartilhar componentes de aplicação entre clientes distintos, mantendo isolamento lógico ou modular dos dados segundo políticas definidas pela Administração, sem possibilidade de acesso cruzado a informações sensíveis.	8	Segurança e Controle de Acesso

AVALIAÇÃO DE CONFORMIDADE DOS REQUISITOS				
Autodeclaração da INTERESSADA			Validação da PRODAM	
Pontos	**Evidência* (indicação de link de internet ou do documento de comprovação enviado)**		**Pontos**	**Parecer Técnico**

Percentual Esperado	%	Pontos (Máximo)	Pontos (Obtidos)	Critério de Qualificação Técnica
70%	0	64	0	Segurança e Controle de Acesso
60%	0	60	0	Arquitetura e Infraestrutura
70%	0	42	0	Integração e Interoperabilidade
50%	0	12	0	Usabilidade e Interface
70%	0	54	0	Inteligência Artificial e Analytics
50%	0	40	0	Gestão de Incidentes e Fluxo Operacional
60%	0	20	0	Compliance e Governança
70%	0	28	0	Dados e Armazenamento
60%	0	24	0	Operação e Monitoramento
Total		**344**	0	

EDITAL DE CHAMAMENTO PÚBLICO PARA SELEÇÃO DE PARCEIRO PRIVADO

ANEXO V - PLANILHA DE QUALIFICAÇÃO TÉCNICA - CAPACIDADE

Item	Requisitos	Motivação/Finalidade	Forma de Demonstração	Critério de Aceitação	Pontuação	Tipo
1	**Capacidade Técnico-Operacional**					
1.1	Experiência prévia na implantação e operação de sistemas críticos	Assegurar que a empresa parceira possua experiência prática técnica e operacional.	Atestado de Capacidade Técnica ou Contratos executados ou em execução emitidos por pessoa jurídica pública ou privada.	Constatação do atestado ou contráto válido, com solução compatível ao objeto de contratação.	10	Capacidade Técnico-Operacional
1.2	Documentação de Operação, Software e Manuais	Assegurar transparência, governança e operação, sustentando processos de compartilhamento de conhecimento e eventuais auditorias.	Documentação técnica mínima contendo especificações, arquitetura, guias de uso e processos operacionais.	Constatação de documento(s) entregues que cubram a requisito solicitado.	10	Capacidade Técnico-Operacional
1.3	Plano de Continuidade Operacional e Recuperação de Desastres (Disaster Recovery)	Assegurar a disponibilidade da plataforma em cenários críticos, preservando a integridade de dados e garantindo a retomada rápida dos serviços essenciais de segurança urbana.	Documentação do plano formal de continuidade de negócios e recuperação de desastres, contendo procedimentos, prazos e níveis de serviço para restabelecimento da plataforma em situações de falha grave, indisponibilidade, corrupção de dados ou desastre natural.	Constatação de documento(s) entregues que cubram a requisito solicitado.	10	Capacidade Técnico-Operacional
1.4	Conformidade com Normas de Segurança Urbana e TIC	Assegurar que a plataforma opere em conformidade com práticas consolidadas de segurança, governança e qualidade, reduzindo riscos operacionais e garantindo integração segura com o ecossistema municipal.	Documentação técnica, políticas internas de segurança da solução, declaração do fabricante confirmando aderência a práticas reconhecidas	Comprovação documental de que a solução adota práticas amplamente aceitas de segurança e tecnologia da informação, condizentes com padrões utilizados pelo setor público e compatíveis com as diretrizes institucionais da Administração.	10	Capacidade Técnico-Operacional
1.5	Processo formal de gestão de incidentes operacionais	Assegurar o controle da operação do serviço, garantindo o acionamento dos agentes necessários para solução, registro da ocorrência e formação de evidências para resposta ao incidente.	Plano documental da gestão de incidentes.	Comprovação documental do plano, contendo processos/fluxos, responsáveis, canais de atendimento de entrada e saída da informação, ponto focal responsável pela operação como um todo e disponibilidade de 24x7 da gestão de incidentes.	10	Capacidade Técnico-Operacional
2	**Capacidade Técnico-Profissional**					
2.1	Possuir em seu quadro de profissionais pelo menos 1 (um) especialista com certificação profissional reconhecida em Proteção de Dados Pessoais (LGPD)	Assegurar que a empresa parceira possua profissional qualificado em proteção de dados pessoais para execução do contrato.	Certificação do profissional e registro de vínculo empregatício ou contrato de prestação de serviço.	Constatação do certificado válido do profissional e do vínculo empregatício ou contrato de prestação de serviço vigente	10	Capacidade Técnico-Profissional
2.2	Possuir em seu quadro de profissionais pelo menos 1 (um) especialista em segurança da informação	Assegurar que a empresa parceira possua profissional qualificado em relação a segurança da informação em projeto crítico análogo.	Currículo resumido com atestado ou declaração de experiência mínima de X anos na área e Y anos em projeto crítico análogo.	Constatação do atestado ou declaração de experiência, com descrição do projeto e currículo resumido	10	Capacidade Técnico-Profissional
2.3	Possuir em seu quadro de profissionais pelo menos 1 (um) arquiteto de solução em nuvem	Assegurar que a empresa parceira possua profissional qualificado em relação a arquitetura de solução em nuvem em projeto crítico análogo.	Currículo resumido com atestado ou declaração de experiência mínima de X anos na área e Y anos em projeto crítico análogo.	Constatação do atestado ou declaração de experiência, com descrição do projeto e currículo resumido	10	Capacidade Técnico-Profissional
2.4	Possuir em seu quadro de profissionais pelo menos 1 (um) especialista em inteligência artificial	Assegurar que a empresa parceira possua profissional qualificado em inteligência artificial, conhecendo o treinamento e processamento.	Currículo resumido com atestado ou declaração de experiência mínima de X anos na área e Y anos em projeto crítico análogo.	Constatação do atestado ou declaração de experiência, com descrição do projeto e currículo resumido	10	Capacidade Técnico-Profissional
3	**Capacidade Técnica Governança**					
3.1	**Requisitos Ambientais**					
3.1.1	Compromisso com o descarte adequado de resíduos e/ou recuperação de recursos, com o combate ao aquecimento global e redução ou compensação da emissão de gases de efeito estufa	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados há pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas.	5	Capacidade Técnica Governança
3.1.2	Compromisso com a eficiência energética e/ou uso de energias renováveis.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados a pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas.	5	Capacidade Técnica Governança
3.2	**Requisitos Sociais**					
3.2.1	Compromisso com a diversidade, equidade e inclusão de grupos minorizados.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados há pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas.	5	Capacidade Técnica Governança
3.2.2	Compromisso com o respeito aos direitos humanos, combate ao trabalho forçado ou compulsório e combate ao trabalho infantil.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados a pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas.	5	Capacidade Técnica Governança
3.3	**Requisitos de Governança**					
3.3.1	Comrpomisso com a boa governança corporativa, com a auditoria, canal de denúncia, código de ética e de conduta e compromisso com a satisfação das partes interessadas.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados a pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas: existência dos documentos descritos, apurações em andamentos.	5	Capacidade Técnica Governança
3.3.2	Compromisso com a integridade e/ou anticorrupção.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados a pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas: existência dos documentos descritos, apurações em andamentos.	5	Capacidade Técnica Governança
3.3.3	Compromisso com a gestão de riscos.	a) Documentos corporativos como certificados, declarações, políticas, normas ou códigos internos aprovados, publicados e implementados a pelo menos 6 (seis) meses; e b) Práticas implementadas como projetos, programas, campanhas, iniciativas, ações etc.	Demonstração do compromisso com o tema por meio dedocumentos corporativos e demonstração das práticas implementadas.	Constatação da implementação das práticas: existência dos documentos descritos, apurações em andamentos.	5	Capacidade Técnica Governança
4	**Certificações**					
4.1	Aderência às Normas ISO/IEC Correspondentes os controles de privacidades alinhados à LGPD	Assegurar que a empresa parceira possua processos de governança e controles de privacidade alinhados à Lei Geral de Proteção de Dados (LGPD).	Documentação, atestado ou certificado que demonstre a aderência à norma.	Constatação do certificado válido ou do atestado, da declaração expressa ou do contrato do processo de certificação, emitidos por entidade certificadora acreditada, considerando as normas ISO/IEC 27001, 27002, 27701.	3	Certificações
4.2	Aderência às Normas ISO/IEC Correspondentes os controles de gestão e risco de segurança	Assegurar que a empresa parceira possua qualidade em processos e sistemas de segurança da informação.	Documentação, atestado ou certificado que demonstre a aderência à norma.	Constatação do certificado válido ou do atestado, da declaração expressa ou do contrato do processo de certificação, emitidos por entidade certificadora acreditada, considerando as normas ISO/IEC 27004, 27005, 27007 e 27032.	3	Certificações
4.3	Aderência às Normas ISO/IEC Correspondentes os controles segurança em nuvem	Assegurar que a empresa parceira possua qualidade em processos e sistemas de segurança da informação hospedados em nuvem.	Documentação, atestado ou certificado que demonstre a aderência à norma.	Constatação do certificado válido ou do atestado, da declaração expressa ou do contrato do processo de certificação, emitidos por entidade certificadora acreditada, considerando as normas ISO/IEC 270017 e 270018.	3	Certificações

4.4	Aderência às Normas ISO/IEC Correspondentes os controles de Continuidade de Negócios	Assegurar que a empresa parceira possua proteção e resposta à incidentes, garantindo continuidade de negócio.	Documentação, atestado ou certificado que demonstre a aderência à norma.	Constatação do certificado válido ou do atestado, da declaração expressa ou do contrato do processo de certificação, emitidos por entidade certificadora acreditada, considerando as normas ISO/IEC 22301 e ISO 9001.	3	Certificações
4.5	Aderência às Normas ISO/IEC Correspondentes os controles gestão de serviços de TI	Assegurar que a empresa parceira possua planejamento, implementação, operação e monitoramento de serviços de TI.	Documentação, atestado ou certificado que demonstre a aderência à norma.	Constatação do certificado válido ou do atestado, da declaração expressa ou do contrato do processo de certificação, emitidos por entidade certificadora acreditada, considerando as normas ISO/IEC 20000-1.	3	Certificações

AVALIAÇÃO DE CONFORMIDADE DOS REQUISITOS

Autodeclaração da INTERESSADA			Validação da PRODAM	
Pontos	**Evidência* (indicação de link de internet ou do documento de comprovação enviado)**		**Pontos**	**Parecer Técnico**

Percentual Esperado	%	Pontos (Máximo)	Pontos (Obtidos)	Critério de Qualificação Técnica
70%	0	50	0	Capacidade Técnico-Operacional
60%	0	40	0	Capacidade Técnico-Profissional
60%	0	35	0	Capacidade Técnica Governança
40%	0	15	0	Certificações
Total		**140**	**0**	

MODELO DE MINUTA DO CONTRATO DE PARCERIA EM OPORTUNIDADE DE NEGÓCIO – PRODAM

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP, empresa pública municipal, regida pela Lei Federal nº 13.303/2016, pela Lei Municipal nº 13.278/2002, inscrita no CNPJ nº 43.076.094/0001-42, com sede na Rua Libero Badaro, 425, São Paulo/SP, doravante denominada PRODAM, representada por seu(s) representante(s) legal(is);

E de outro lado,

XXXXX, inscrita no CNPJ nº XXXXX, com sede na XXXXXX, doravante denominada PARCEIRA;

As quais, em conjunto, serão denominadas PARCEIRAS.

Celebram o presente Contrato de Parceria em Oportunidade de Negócio, nos termos do art. 28, §3º, II, e §4º da Lei Federal nº 13.303/2016, do Regulamento de Parcerias em Oportunidades de Negócio da PRODAM – RPON-PRODAM (versão 19.11.25), bem como pelas normas do Direito Privado, mediante as cláusulas a seguir.

CLÁUSULA 1 – DEFINIÇÕES

1.1. Para fins deste Contrato Associativo de Parceria em Oportunidade de Negócio SMARTSAMPA, os termos abaixo, quando grafados com inicial maiúscula, no singular ou no plural, terão os seguintes significados, complementando as definições constantes do Regulamento de Parcerias em Oportunidades de Negócio da PRODAM-SP – RPON-PRODAM:

I – PRODAM: a EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP, empresa pública municipal, regida pela Lei Federal nº 13.303/2016, pela Lei Municipal nº 13.278/2002, por seu Estatuto Social, pelo RPON-PRODAM e demais normas internas;

II – PARCEIRA: a pessoa jurídica privada que celebra o presente Contrato com a PRODAM, na qualidade de agente econômico selecionado nos termos do RPON-PRODAM, para atuar em conjunto na Oportunidade de Negócio SMARTSAMPA;

III – PARCEIRAS: denominação conjunta da PRODAM e da PARCEIRA;

IV – Oportunidade de Negócio (ON): estrutura formal de colaboração prevista no Regulamento de Parcerias da PRODAM (RPON-PRODAM), destinada ao desenvolvimento, evolução, implantação ou exploração conjunta de soluções tecnológicas, digitais ou inovadoras. A ON constitui modelo associativo orientado a resultados, dotado de governança própria, Matriz de

Riscos, Plano da Oportunidade de Negócio (PNO), Plano de Negócio da Parceria (PNPO) e demais instrumentos que organizam sua execução.

A Oportunidade de Negócio:

a) estabelece visão estratégica, objetivos, entregas e responsabilidades das PARCEIRAS;
b) organiza a alocação de riscos, aportes e participações técnicas;
c) estrutura modelo econômico e possibilidades de exploração externa;
d) define o ciclo de vida da solução e a evolução de seus módulos;
e) não gera relação de prestação de serviços ou contraprestação financeira entre as PARCEIRAS;
f) constitui ambiente regulado de inovação, interoperabilidade e desenvolvimento compartilhado;
g) integra e vincula todos os documentos estruturantes da parceria (PNPO, PNO, Matriz de Riscos e demais anexos).

Parágrafo único. Neste Contrato, o SMARTSAMPA é a Oportunidade de Negócio de referência, sendo tratado como ON para todos os efeitos.

V – Oportunidade de Negócio SMARTSAMPA ou simplesmente SMARTSAMPA: solução urbana digital integrada, modular e escalável, concebida como plataforma estruturante de serviços municipais inteligentes, destinada a apoiar a gestão pública, promover a transformação digital da cidade de São Paulo e oferecer funcionalidades avançadas para cidadãos, empresas e órgãos governamentais. O SMARTSAMPA compreende:

a) ecossistema tecnológico interoperável, composto por módulos, APIs, conectores, integrações e serviços digitais compartilháveis;
b) infraestrutura lógica e arquitetônica, orientada a dados, segurança, governança e padrões modernizados de cidades inteligentes;
c) camada de serviços urbanos voltada à mobilidade, atendimento digital, participação social, gestão territorial, monitoramento urbano e demais funcionalidades definidas no PNO;
d) módulos evolutivos, que podem ser ampliados, substituídos ou aperfeiçoados conforme as necessidades da Administração Pública;
e) ambiente de inovação contínua, apto a incorporar novas tecnologias, algoritmos, modelos analíticos, inteligência artificial e serviços conectados;
f) ativo tecnológico estratégico da PRODAM, destinado à exploração externa, observada a política de parcerias, as regras de propriedade intelectual e o modelo econômico definido neste Contrato.

Parágrafo único. O SMARTSAMPA é tratado neste Contrato como Oportunidade de Negócio de natureza urbana, tecnológica e inovadora, podendo ser expandido, evoluído ou reconfigurado mediante deliberação da governança da ON e atualização do PNO.

VI – Agente Econômico: qualquer pessoa física ou jurídica que, em tese, possa vir a celebrar parceria ou outra forma associativa em oportunidades de negócio com a PRODAM, na forma do RPON-PRODAM;

VII – Interessado(a): pessoa física ou jurídica que tenha manifestado interesse em firmar contrato de parceria com a PRODAM relativamente à Oportunidade de Negócio, em procedimento de chamamento público ou diálogo com agentes econômicos;

VIII – Contrato de Parceria em Oportunidade de Negócio ou Contrato Associativo: instrumento jurídico de natureza predominantemente privada, típico ou atípico, pelo qual se disciplina a atuação conjunta das PARCEIRAS na Oportunidade de Negócio SMARTSAMPA, sem constituição de sociedade e sem vínculo de prestação de serviços entre elas;

IX – Avaliação Preliminar da Oportunidade de Negócio (APON): análise inicial, não exaustiva, realizada pela PRODAM sobre a conveniência e a viabilidade da Oportunidade de Negócio SMARTSAMPA, quanto à aderência ao objeto social da PRODAM e às projeções preliminares de mercado, formalizada por meio do Relatório de Avaliação Preliminar (RAP);

X – Relatório de Avaliação Preliminar (RAP): documento elaborado pela PRODAM que formaliza a APON, contendo, no mínimo, a descrição sumária da Oportunidade de Negócio, a aderência à atuação da PRODAM, projeções iniciais de mercado e recomendação fundamentada pelo prosseguimento ou arquivamento da parceria;

XI – Plano de Negócio Preliminar da Oportunidade (PNPO): documento-base que estrutura preliminarmente a Oportunidade de Negócio SMARTSAMPA, descrevendo objetivos gerais, mapeamento inicial de agentes econômicos, alternativas tecnológicas, aspectos concorrenciais, diretrizes de governança e avaliação de riscos, servindo como referência para a etapa de seleção do parceiro;

XII – Plano de Negócio da Oportunidade (PNO): documento-base definitivo de estruturação da Oportunidade de Negócio SMARTSAMPA, que detalha objetivos, escopo, estratégia de inserção no mercado, modelo econômico-financeiro, responsabilidades das PARCEIRAS, indicadores de desempenho, regime de propriedade intelectual, compartilhamento de resultados e regras de saída, compondo referência obrigatória para a execução deste Contrato;

XIII – Matriz de Riscos: documento integrante do PNO, acostado a este Contrato como Anexo C, que identifica, qualifica e aloca os riscos intrínsecos e extrínsecos da Oportunidade de Negócio SMARTSAMPA entre as PARCEIRAS, bem como suas medidas mitigadoras;

XIV – Diálogos com Agentes Econômicos: procedimentos de interação da PRODAM com agentes econômicos, tais como procedimentos de manifestação de interesse privado, tomadas de subsídios, reuniões participativas, roadshows, pedidos de informação (RFI), pedidos de proposta (RFP), provas de conceito (POC), provas de valor (POV), audiências e consultas públicas, nos termos do RPON-PRODAM;

XV – Cliente(s): pessoas físicas ou jurídicas, públicas ou privadas, que venham a contratar produtos, serviços ou soluções decorrentes da Oportunidade de Negócio SMARTSAMPA, mediante instrumentos próprios celebrados com a PRODAM, com a PARCEIRA ou com ambas,

conforme o modelo de negócio definido no PNO;

XVI – Informações Sigilosas: quaisquer dados, documentos, relatórios, códigos, especificações técnicas, planos, estudos, estratégias comerciais, informações de clientes, segredos de negócio ou quaisquer outras informações, em qualquer formato ou suporte, que sejam classificadas como confidenciais por qualquer das PARCEIRAS ou que, pela sua natureza, devam ser assim consideradas, inclusive aquelas classificadas como sigilosas nos termos do Anexo D e da legislação aplicável;

XVII – Dados Pessoais e Dados Pessoais Sensíveis: informações assim definidas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), tratadas no âmbito da Oportunidade de Negócio SMARTSAMPA nos termos deste Contrato, do Anexo A – Tratamento de Dados Pessoais e do Anexo E – Relatório de Impacto de Proteção de Dados;

XVIII – Código de Conduta e Integridade da PRODAM, Política Anticorrupção da PRODAM e Programa de Integridade e Boas Práticas (PIBP): instrumentos normativos internos da PRODAM que estabelecem princípios, diretrizes e regras de conduta ética, integridade e prevenção à corrupção, de observância obrigatória pelas PARCEIRAS na execução deste Contrato;

XIX – Gestor de Contrato: empregado(a) da PRODAM formalmente designado(a) para coordenar a gestão e acompanhar a execução deste Contrato, inclusive quanto à interface com a PARCEIRA, à adoção de providências corretivas e à proposição de aditivos, nos termos do RPON-PRODAM e das normas internas;

XX – Fiscal(ais) de Parceria: empregado(s) da PRODAM formalmente designado(s) para fiscalizar o cumprimento das obrigações assumidas neste Contrato, especialmente nos aspectos técnicos e administrativos, registrando ocorrências e subsidiando o Gestor de Contrato;

XXI – Gestor de Produto: empregado(a) da PRODAM responsável pela visão de negócio, pela estratégia, pelo roadmap e pelo equilíbrio econômico-financeiro do produto/solução associada à Oportunidade de Negócio SMARTSAMPA, conforme designação interna.

1.2. Em caso de lacunas ou dúvidas de interpretação quanto a quaisquer termos aqui empregados, prevalecerá a definição constante do RPON-PRODAM e, supletivamente, da legislação aplicável.

1.3. Integram este Contrato, para todos os fins, como se nele estivessem transcritos, além dos Anexos aqui mencionados, os seguintes documentos, desde que aprovados no processo administrativo correspondente à Oportunidade de Negócio SMARTSAMPA:

I – Plano de Negócio da Oportunidade (PNO), inclusive sua Matriz de Riscos;
II – atos de homologação do processo de seleção da PARCEIRA;
III – eventuais Termos de Confidencialidade e Acordos específicos de teste, prova de conceito ou prova de valor, celebrados entre as PARCEIRAS.

1.4. Em caso de divergência entre este Contrato e os documentos referidos no item 1.3, prevalecerá:

I – em matéria de conformidade com a Lei nº 13.303/2016 e com o RPON-PRODAM, a interpretação que melhor atenda aos seus princípios e disposições;
II – nas demais matérias, a ordem de prevalência será definida no PNO, podendo as PARCEIRAS, em caso de dúvida, firmar termo aditivo esclarecedor.

CLÁUSULA 2 – DO OBJETO

2.1. O presente Contrato Associativo tem por objeto a cooperação estratégica, técnica, tecnológica, operacional e comercial entre as PARCEIRAS para a implementação, evolução, manutenção, operação, ampliação, gestão, integração, comercialização e exploração conjunta da Oportunidade de Negócio denominada SMARTSAMPA, concebida como plataforma urbana inovadora, modular, interoperável e orientada a dados, voltada à transformação digital da cidade de São Paulo e de demais localidades interessadas.

2.1.1 – Natureza urbana, inovadora e transversal do objeto

Para todos os fins, considera-se que a solução SMARTSAMPA consiste em:

I – Plataforma urbana inteligente, apta a integrar informações, serviços públicos e privados, sistemas legados, bases cadastrais, sensores, APIs, IoT e dados territoriais do Município;

II – Solução tecnológica inovadora, em constante evolução, incorporando práticas de analytics, inteligência artificial, interoperabilidade, automação urbana, gestão de casos, comunicação digital e outras tecnologias emergentes;

III – Infraestrutura estratégica de transformação digital, contribuindo para melhoria de políticas públicas, gestão territorial, mobilidade, vigilância ambiental, emergência urbana, serviços ao cidadão e iniciativas correlatas;

IV – Ferramenta de integração digital de serviços urbanos, promovendo eficiência, acessibilidade, conectividade e participação cidadã;

V – Sistemas digitais escaláveis e replicáveis, apto a ser comercializado com órgãos públicos, entidades privadas, concessionárias e demais agentes econômicos, conforme o PNO.

2.2 – Abrangência da colaboração entre as PARCEIRAS

A atuação conjunta das PARCEIRAS compreenderá, de forma não exaustiva:

a) execução técnica, operacional e comercial do PNO da Oportunidade de Negócio SMARTSAMPA;

b) desenvolvimento e evolução incremental das funcionalidades;
c) integração com plataformas municipais, bases de dados, cadastros técnicos e sistemas legados;
d) operação compartilhada da solução, conforme modelo definido no PNO;
e) ações estratégicas de inserção da solução no mercado;
f) elaboração de materiais técnicos, protótipos, provas de conceito, roadmaps, releases e incrementos tecnológicos;
g) participação conjunta em iniciativas de inovação, testes controlados, sandbox regulatórios e projetos-piloto, quando aplicável;
h) atendimento às métricas de desempenho e indicadores definidos no PNO;
i) identificação contínua de oportunidades de melhoria, expansão e novos módulos do sistema SMARTSAMPA.

2.3 – Natureza jurídica da relação

2.3.1. O presente contrato possui natureza estritamente associativa, não configurando:

I – prestação de serviços por qualquer das PARCEIRAS à outra;
II – relação de consumo;
III – relação de representação comercial;
IV – terceirização ou intermediação de mão de obra;
V – sociedade, joint venture societária ou consórcio formal.

2.3.2. Cada PARCEIRA permanece autônoma, independente e responsável por seus próprios recursos, obrigações fiscais, trabalhistas e previdenciárias.

2.4 – Não exclusividade e ausência de obrigação de demanda

2.4.1. A associação aqui disciplinada não implica exclusividade, salvo disposição expressa futura mediante aditivo.

2.4.2. A celebração deste contrato não constitui garantia de demanda, receita, faturamento mínimo ou contratação por terceiros, estando os resultados vinculados exclusivamente à exploração conjunta de mercado, conforme o PNO.

2.5 – Documentos que especificam o objeto

2.5.1. A descrição técnica, funcional, arquitetural e organizacional do objeto encontra-se detalhada nos seguintes documentos, que integram este Contrato:

I – PNPO – Plano de Negócio Preliminar da Oportunidade;
II – PNO – Plano de Negócio da Oportunidade, incluindo seus anexos, métricas, roadmap, arquitetura, modelo econômico-financeiro e responsabilidades;
III – Anexo B – Detalhamento Técnico da Solução SMARTSAMPA;
IV – Anexo B.1 – Descrição da Solução e de seus Módulos;

V – Anexo C – Matriz de Riscos da Oportunidade de Negócio.

2.6 – Finalidade e objetivos estratégicos da parceria

2.6.1. As PARCEIRAS reconhecem que a parceria tem por finalidades:

I – promover a transformação digital do Município de São Paulo e de outras localidades, mediante solução inovadora aplicada ao contexto urbano;
II – gerar valor público, eficiência operacional e impacto social positivo;
III – fortalecer o papel da PRODAM como empresa pública de inovação e tecnologia urbana;
IV – fomentar o sistema de inovação municipal e regional;
V – permitir a exploração conjunta, sustentável e transparente de mercado, conforme princípios da Lei nº 13.303/2016.

2.7 – Caráter evolutivo e experimental da solução

2.7.1. A SMARTSAMPA é uma solução dinâmica, passível de:

a) evolução tecnológica contínua;
b) aprimoramento funcional;
c) criação de novos módulos ou camadas;
d) integração com tecnologias emergentes;
e) adaptação regulatória e urbana.

2.7.2. A evolução é parte indissociável do objeto, devendo as PARCEIRAS assegurar que:

I – a solução se mantenha inovadora;
II – siga padrões atualizados de segurança e interoperabilidade;
III – incorpore melhorias validadas no processo administrativo da ON.

CLÁUSULA 3 – DAS OBRIGAÇÕES

3.1 – Obrigações Comuns

Sem prejuízo das demais disposições deste Contrato e dos documentos integrantes da Oportunidade de Negócio SMARTSAMPA, constituem obrigações de ambas as PARCEIRAS:

I – atuar em cooperação técnica, operacional e estratégica para execução, evolução e exploração da Oportunidade de Negócio SMARTSAMPA, conforme PNPO, PNO, Matriz de Riscos e demais documentos aplicáveis;

II – assegurar a execução integrada, ética e transparente das atividades relacionadas à solução urbana SMARTSAMPA, observando o RPON-PRODAM, a Lei nº 13.303/2016, as normas internas aplicáveis e a legislação vigente;

III – participar de reuniões técnicas, de governança e grupos de trabalho, garantindo apoio técnico e operacional às deliberações necessárias ao desenvolvimento da solução;

IV – zelar pela integridade, confidencialidade, rastreabilidade e segurança da informação, inclusive no tratamento de dados pessoais e no uso de bases territoriais do Município;

V – adotar práticas de gestão de risco, observando a Matriz de Riscos da ON e seus desdobramentos, comunicando imediatamente eventuais eventos críticos, incidentes ou vulnerabilidades;

VI – cooperar na elaboração, atualização e execução de evolução da solução SMARTSAMPA, garantindo alinhamento contínuo com o PNO;

VII – atender às solicitações de informações, documentos e subsídios técnicos que se façam necessários à governança da ON, auditorias internas/externas, diligências ou verificações de conformidade;

VIII – responder, nos limites de suas responsabilidades, por danos decorrentes de ações ou omissões próprias, de seus empregados ou de terceiros sob sua coordenação;

IX – observar padrões técnicos, de interoperabilidade, de qualidade e de segurança definidos no PNO, na Matriz de Riscos e em normativos da PRODAM-SP.

3.2 – Obrigações Específicas da PARCEIRA

Constituem obrigações específicas da PARCEIRA:

I – executar todas as atividades técnicas, tecnológicas e operacionais sob sua responsabilidade, conforme definidos no PNO, anexos técnicos e decisões de governança;

II – garantir a conformidade tecnológica das soluções, módulos, componentes, integrações, APIs, algoritmos, serviços e funcionalidades sob sua responsabilidade, assegurando desempenho, escalabilidade, interoperabilidade e continuidade operacional;

III – fornecer equipe qualificada, com experiência comprovada nas tecnologias e metodologias aplicáveis ao SMARTSAMPA, mantendo-a dimensionada para atender as obrigações deste Contrato;

IV – entregar artefatos técnicos, testes, relatórios, protótipos, provas de conceito, provas de valor, análises, especificações e integrações, conforme requisitos do PNO;

V – manter atualizadas as documentações técnica e funcional da solução, incluindo arquitetura, APIs, integrações, diagramas, manuais e procedimentos operacionais;

VI – notificar imediatamente a PRODAM sobre falhas críticas, incidentes de segurança, riscos tecnológicos ou operacionais, bem como sobre qualquer fato que possa comprometer o desempenho da solução urbana;

VII – atuar com aderência integral às políticas de integridade, compliance, anticorrupção, segurança da informação e governança de dados da PRODAM, inclusive submetendo-se às avaliações de integridade previstas no RPON-PRODAM;

VIII – manter-se adimplente com todas as suas obrigações fiscais, regulatórias, trabalhistas e previdenciárias, não podendo transferir às PARCEIRAS qualquer responsabilidade decorrente dessas obrigações;

IX – prestar suporte técnico e esclarecimentos que se façam necessários à exploração comercial do SMARTSAMPA, incluindo demonstrações, apresentações, reuniões e participação em eventos técnicos coordenados pela PRODAM;

X – abster-se de utilizar a marca SMARTSAMPA, ou qualquer marca associada ao sistema digital do Município, sem autorização expressa da PRODAM.

3.3 – Obrigações Específicas da PRODAM

Compete exclusivamente à PRODAM:

I – atuar como agente articulador institucional perante órgãos públicos, entidades privadas, concessionárias, munícipes e demais atores do sistema urbano, promovendo a inserção e expansão do SMARTSAMPA;

II – coordenar a governança da Oportunidade de Negócio, designando Gestor do Contrato, Fiscal(is) e Gestor de Produto, além de consolidar decisões internas necessárias à evolução da solução;

III – realizar a gestão comercial e estratégica da solução, incluindo estudos de mercado, prospecção de clientes, intermediação de negócios e condução de negociações;

IV – fornecer infraestrutura tecnológica, conectividade, interoperabilidade, ambientes, dados, bases territoriais, cadastros e integrações, quando sob sua responsabilidade;

V – centralizar o atendimento de demandas regulatórias, institucionais e normativas, quando relacionadas ao uso de dados municipais, interfaces com órgãos públicos ou requisitos legais;

VI – gerenciar o processo administrativo da ON, incluindo PNPO, PNO, decisões de homologação, anexos técnicos, atas de reuniões, Comunicações Oficiais e documentos de governança;

VII – supervisionar os indicadores de desempenho, assegurando aderência aos padrões

estabelecidos no PNO e orientando eventuais medidas corretivas;

VIII – proceder à retenção de tributos e demais encargos aplicáveis sobre eventuais repasses à PARCEIRA, nos termos da legislação vigente;

IX – promover a atualização da Matriz de Riscos, sempre que necessário à manutenção da segurança, integridade e continuidade da solução.

3.4 – Vedações Comuns às PARCEIRAS

É vedado às PARCEIRAS:

I – adotar práticas que comprometam a integridade, a governança, a transparência ou a rastreabilidade da ON;
II – implementar funcionalidades, integrações ou módulos que contrariem o PNO ou que não tenham sido validados na governança da ON;
III – compartilhar informações sigilosas ou dados pessoais em desacordo com este Contrato, com o Anexo D e com a LGPD;
IV – comprometer a continuidade operacional da solução por negligência, imperícia, imprudência ou falta de governança;
V – praticar atos que possam gerar conflito de interesse, vantagem indevida ou violação às normas de integridade.

CLÁUSULA 4 – DO ARCABOUÇO NORMATIVO APLICÁVEL

4.1. O presente Contrato Associativo, bem como todos os atos, decisões, responsabilidades e obrigações decorrentes da Oportunidade de Negócio SMARTSAMPA, serão regidos pela legislação brasileira aplicável e pelos normativos internos da PRODAM, observando-se, de forma conjunta e complementar, o seguinte arcabouço jurídico-normativo:

I – LEGISLAÇÃO FEDERAL, ESTADUAL E MUNICIPAL APLICÁVEL

a) Lei Federal nº 13.303/2016 – Lei das Empresas Estatais, especialmente no que se refere aos princípios, regras e diretrizes aplicáveis à gestão pública empresarial, às parcerias, às formas associativas e à governança corporativa das empresas públicas;

b) Lei Federal nº 10.973/2004 (Lei de Inovação), quando aplicável à execução de atividades de pesquisa, desenvolvimento, inovação, transferência tecnológica e exploração tecnológica conjunta;

c) Lei Federal nº 12.846/2013 (Lei Anticorrupção) e seus regulamentos, aplicável integralmente às PARCEIRAS no âmbito deste Contrato;

d) Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), regulando todo

tratamento de dados pessoais realizado no contexto da solução inovadora urbana SMARTSAMPA;

e) Código Civil Brasileiro, para todas as situações de natureza privada, supletivamente;

f) legislação municipal aplicável às atividades de tecnologia, inovação, modernização administrativa e governo digital, incluindo normas de dados territoriais, integração de sistemas e interoperabilidade municipal.

II – NORMATIVOS INTERNOS DA PRODAM-SP

4.2. As PARCEIRAS reconhecem que este Contrato se submete integralmente aos normativos internos da PRODAM, dentre os quais:

I – Regulamento de Parcerias em Oportunidades de Negócio da PRODAM – RPON-PRODAM (versão 19.11.25), que constitui norma-matriz deste instrumento, disciplinando a formação, análise, seleção, homologação, formalização e execução da parceria SMARTSAMPA;

II – Estatuto Social da PRODAM e suas alterações posteriores;

III – Código de Ética e Conduta da PRODAM, aplicável a todos os empregados e colaboradores envolvidos;

IV – Política Anticorrupção, Política de Integridade e demais normas que integram o Programa de Integridade e Boas Práticas (PIBP);

V – Políticas e Normas de Segurança da Informação, Cibersegurança, Gestão de Dados, Interoperabilidade, Conectividade Municipal e demais regulamentos técnicos que disciplinem requisitos de segurança, proteção, classificação e uso de dados estratégicos do Município;

VI – Normas internas de Gestão de Contratos, Aditivos, Fiscalização, Governança, Auditoria e Controles Internos;

VII – Manuais, guias, diretrizes técnicas e padrões de arquitetura e interoperabilidade definidos pelo sistema PRODAM-SP.

III – DOCUMENTOS ESTRUTURANTES DA OPORTUNIDADE DE NEGÓCIO SMARTSAMPA

4.3. Para todos os fins, constituem parte integrante do arcabouço normativo deste Contrato e vinculam as PARCEIRAS:

I – o Relatório de Avaliação Preliminar (RAP), produzido na etapa de APON;
II – o PNPO – Plano de Negócio Preliminar;
III – o PNO – Plano de Negócio da Oportunidade, documento central de governança e execução,

incluindo seus anexos;
IV – a Matriz de Riscos da ON;
V – demais documentos e decisões formalmente registrados no processo administrativo da SUSEI/PRODAM relacionadas à ON SMARTSAMPA.

IV – ORDEM DE PREVALÊNCIA ENTRE NORMAS E DOCUMENTOS

4.4. Em caso de conflito entre este Contrato, seus Anexos e os demais documentos integrantes da ON, observar-se-á a seguinte ordem de prevalência:

I – a legislação federal aplicável, especialmente a Lei nº 13.303/2016 e a LGPD;
II – o RPON-PRODAM;
III – o presente Contrato Associativo;
IV – o PNO – Plano de Negócio da Oportunidade;
V – a Matriz de Riscos da ON;
VI – o PNPO;
VII – demais documentos acessórios.

4.5. Os documentos técnicos, funcionais, de arquitetura e de interoperabilidade serão interpretados à luz da estratégia urbana, da vocação inovadora e do caráter evolutivo da solução SMARTSAMPA, conforme definido no PNO.

V – REGIME JURÍDICO E INTERPRETAÇÃO

4.6. O presente Contrato reger-se-á predominantemente pelo Direito Privado, nos termos do art. 68 da Lei nº 13.303/2016, sem prejuízo da aplicação de normas de compliance, controle, integridade, governança e transparência previstas na legislação e nas normas internas da PRODAM.

4.7. A interpretação das cláusulas deverá observar, sempre:

I – os princípios da administração pública, incluindo legalidade, isonomia, motivação, eficiência, razoabilidade, publicidade e interesse público;
II – os vetores de interpretação do RPON-PRODAM, como governança, segurança jurídica, inovação prudente, rastreabilidade e agilidade;
III – o caráter associativo, colaborativo e inovador da parceria;
IV – a finalidade pública da solução SMARTSAMPA e seu impacto urbano.

CLÁUSULA 5 – GOVERNANÇA, SEGREGAÇÃO DE FUNÇÕES E RASTREABILIDADE

5.1. A execução da Oportunidade de Negócio SMARTSAMPA observará o modelo de governança corporativa, integridade, transparência e rastreabilidade estabelecido pela PRODAM-SP e pelo RPON-PRODAM, garantindo que todas as decisões, atos e interações sejam integralmente registradas, controladas e auditáveis.

5.2 – Princípios de Governança da ON SMARTSAMPA

A governança desta Oportunidade de Negócio reger-se-á pelos seguintes princípios:

I – Transparência: todas as decisões, documentos, interações, riscos e deliberações devem ser formalmente registradas no processo administrativo eletrônico correspondente;

II – Rastreabilidade: todos os atos da ON devem ser identificáveis, auditáveis e recuperáveis a qualquer tempo, permitindo reconstrução clara da linha decisória;

III – Accountability: cada PARCEIRA assume responsabilidade por suas ações, decisões e informações prestadas;

IV – Colegiado: decisões estratégicas e evolutivas devem ser tomadas em governança conjunta, respeitando-se as atribuições da PRODAM como líder da ON;

V – Padronização e Conformidade: observância obrigatória às normas internas da PRODAM, ao RPON-PRODAM e às políticas de integridade;

VI – Segurança Jurídica e Técnica: decisões devem ser motivadas tecnicamente, com base em critérios transparentes, dados confiáveis e pareceres pertinentes.

5.3 – Estrutura de Governança da Oportunidade de Negócio

A ON será governada pela seguinte estrutura de papéis e responsabilidades:

I – Gestor da Parceria (PRODAM)

Designado pela PRODAM, com atribuições de:

a) coordenar a execução do Contrato Associativo;
b) convocar e conduzir reuniões de governança;
c) comunicar riscos, incidentes e necessidades de deliberação;
d) validar entregas críticas e marcos de evolução;
e) garantir aderência ao PNPO, ao PNO e à Matriz de Riscos;
f) propor aditivos, ajustes ou redirecionamentos estratégicos.

II – Fiscal(is) da Parceria (PRODAM)

Técnicos designados com função de:

a) fiscalizar o cumprimento das obrigações da PARCEIRA;
b) analisar evidências, relatórios, artefatos e entregas;
c) registrar todas as ocorrências de conformidade e inconformidade;

d) subsidiar o Gestor com pareceres técnicos.

III – Gestor de Produto (PRODAM)

Responsável por:

a) conduzir a visão estratégica e a evolução funcional da solução SMARTSAMPA;
b) manter o roadmap atualizado;
c) assegurar aderência tecnológica e inovadora com o sistema municipal;
d) acompanhar indicadores de impacto urbano e de valor público.

V – Comitê de Governança da ON

Composto por representantes técnicos e estratégicos de ambas as PARCEIRAS, com atribuições de:

a) deliberar sobre mudanças de escopo, priorização e evolução;
b) monitorar riscos e incidentes críticos;
c) validar módulos, integrações e componentes estratégicos;
d) promover alinhamento com diretrizes de cidade inteligente e inovação.

5.4 – Segregação de Funções (arts. 7º e 20 do RPON-PRODAM)

5.4.1. Para assegurar a integridade e reduzir riscos, devem estar segregadas:

I – funções de planejamento, decisão, execução e controle;
II – atividades de análise técnica, parecer jurídico, gestão de contrato e auditoria;
III – funções desempenhadas por empregados ou representantes que, em qualquer hipótese, possam gerar conflito de interesse real, potencial ou aparente.

5.4.2. Nenhum agente da PRODAM ou da PARCEIRA poderá, simultaneamente:

a) decidir e aprovar atos que tenham ele próprio executado;
b) fiscalizar atividades de sua própria responsabilidade;
c) influenciar deliberações quando houver conflito de interesses.

5.5 – Rastreabilidade e Documentação Obrigatória

5.5.1. Todas as interações, reuniões, decisões, validações e entregas devem ser registradas por meio de:

I – atas de reunião;
II – relatórios técnicos;
III – pareceres e análises de risco;
IV – comunicações oficiais via processo eletrônico da PRODAM;

V – controle de versões sobre artefatos, integrações e módulos;
VI – logs de segurança, auditoria e rastreamento de operações críticas.

5.5.2. Todo documento técnico relevante deverá conter:

a) responsável pela elaboração;
b) data e hora;
c) versão;
d) justificativa técnica;
e) relação com itens do PNPO, PNO ou Matriz de Riscos.

5.6 – Governança da Inovação

A governança da inovação deve observar:

I – processos de validação incremental das funcionalidades;
II – compatibilidade com padrões internacionais de cidades inteligentes (ex.: ISO 37120, 37122, 37123), quando aplicável;
III – integração com políticas públicas municipais de inovação e governo digital;
IV – princípios de inovação prudente (art. 2º, RPON-PRODAM);
V – uso responsável de algoritmos, IA, dados e automação.

5.7 – Transparência e Publicidade

5.7.1. As decisões obrigatórias serão registradas no processo administrativo, com publicidade conforme o RPON-PRODAM.

5.7.2. Informações sigilosas e dados protegidos seguirão classificação conforme o Anexo D e os normativos de segurança da PRODAM.

5.8 – Auditoria e Controle

5.8.1. A PARCEIRA admite auditorias:

I – da PRODAM;
II – da Controladoria Geral do Município;
III – do TCM-SP;
IV – do Ministério Público;
V – órgãos de controle interno e externo autorizados.

5.8.2. A PARCEIRA deverá fornecer prontamente todas as informações solicitadas.

CLÁUSULA 6 – CRONOGRAMAS

6.1. A execução da Oportunidade de Negócio SMARTSAMPA observará o Cronograma Executivo definido no PNO – Plano de Negócio da Oportunidade, compreendendo marcos, entregas, fases, indicadores e dependências técnicas.

6.2. O cronograma será composto por fases sequenciais e interdependentes, sem prejuízo de execuções paralelas quando tecnicamente justificável, sendo composto, no mínimo, pelas seguintes etapas:

I – Etapa 1: Estruturação e Consolidação Inicial da ON (até 30 dias)

a) alinhamento técnico e estratégico entre as PARCEIRAS;
b) instalação dos comitês, governanças e grupos de trabalho previstos neste Contrato;
c) definição final dos artefatos iniciais, escopos de integração, prioridades e roadmap mínimo;
d) validação da infraestrutura necessária para início das atividades;
e) elaboração ou atualização inicial da Matriz de Riscos da ON.

II – Etapa 2: Implantação Inicial da Solução (até 90 dias)

a) implementação da versão mínima funcional ou versão inicial definida no PNO;
b) integração dos primeiros módulos essenciais e funcionalidades críticas;
c) testes de desempenho, segurança e interoperabilidade;
d) validação técnica pelo Comitê de Governança;
e) entrega de documentação técnica, manuais, APIs e especificações da fase inicial.

III – Etapa 3: Operação Assistida e Estabilização (período de 30 a 120 dias)

a) operação assistida do sistema SMARTSAMPA;
b) acompanhamento intensivo de indicadores e métricas de desempenho;
c) ajustes, correções e estabilização funcional;
d) entrega de relatórios periódicos, logs e evidências de conformidade;
e) avaliação conjunta de riscos e redefinição de prioridades do roadmap.

IV – Etapa 4: Expansão Funcional e Comercial

a) desenvolvimento incremental de novos módulos, camadas, integrações e funcionalidades;
b) expansão para novos públicos, parceiros, agentes econômicos e clientes;
c) ações comerciais, apresentações, demonstrações e prospecção conjunta;
d) atualizações de segurança, dados, APIs, arquitetura e padrões core;
e) evolução constante com base em indicadores de impacto urbano e valor público.

V – Etapa 5: Evolução Tecnológica Contínua e Inovação Permanente

a) adoção de tecnologias emergentes (IA, visão computacional, IoT, big data, analytics, open data etc.);
b) adequação da solução às políticas municipais e normas internacionais de smart cities;

c) inclusão de módulos derivados de necessidades institucionais e urbanas;
d) participação em ambientes controlados de teste ou sandboxes, quando aplicável;
e) revisão periódica da Matriz de Riscos e de sua mitigação tecnológica.

VI – Etapa 6: Atualizações, Revisões e Governança de Cronograma

6.3. A evolução do cronograma observará:

I – revisões trimestrais ou em periodicidade inferior, se assim definir o Comitê de Governança;
II – ajustes que se façam necessários por razões técnicas, operacionais, urbanas ou estratégicas;
III – registro obrigatório de todas as alterações no processo administrativo da ON;
IV – manutenção das justificativas técnicas e pareceres necessários para ajustes.

6.4. Qualquer alteração substancial do cronograma deverá ser:

a) tecnicamente motivada;
b) validada pelo Comitê de Governança;
c) registrada pelo Gestor da Parceria;
d) compatível com o PNO e com a Matriz de Riscos atualizada.

VII – Natureza Dinâmica e Evolutiva do Cronograma

6.5. Poderá ser estabelecido um cronograma específico para atendimento de proposta comercial apresentada a potencial cliente, desde que:

I – seja elaborado conjuntamente pelas PARCEIRAS;
II – observe o PNO, a Matriz de Riscos e a governança da ON;
III – se restrinja às entregas, marcos e atividades vinculadas à comercialização externa do SMARTSAMPA;
IV – não altere o cronograma-base ou comprometa obrigações essenciais da ON;
V – seja formalmente registrado no processo administrativo da oportunidade vinculada ao cliente.

Parágrafo único. O cronograma específico terá finalidade comercial e operacional e não implicará, por si só, alteração deste Contrato ou do PNO, salvo se expressamente deliberado pela governança da ON.

6.6. Ajustes no cronograma não caracterizam aditivo contratual, desde que não impliquem:

I – alteração de objeto;
II – modificação de responsabilidade;
III – transferência indevida de riscos;
IV – violação ao RPON-PRODAM.

VIII – Marcos de Aprovação e Aceite

6.7. Cada etapa deverá ser acompanhada de Marco de Aprovação, contendo:

a) objetivos da etapa;
b) entregas e artefatos obrigatórios;
c) critérios de aceite;
d) evidências documentais;
e) parecer do Fiscal;
f) homologação pelo Gestor da Parceria.

6.8. O aceite parcial ou condicionado poderá ser concedido mediante plano de ação corretiva registrado no processo da ON.

IX – Indicadores Temporais

6.9. Os prazos e marcos deverão estar alinhados aos indicadores temporais previstos no PNO.

CLÁUSULA 7 – INTEGRIDADE, COMPLIANCE E DUE DILIGENCE

7.1 – Princípios Gerais

7.1.1. A execução deste Contrato deverá observar, integralmente, os princípios de ética, integridade, transparência, governança, prevenção à corrupção, responsabilidade corporativa, conformidade regulatória e diligência no trato da coisa pública, nos termos:

I – da Lei nº 13.303/2016;
II – da Lei nº 12.846/2013 e seus regulamentos;
III – da LGPD – Lei nº 13.709/2018;
IV – da legislação penal e anticorrupção aplicável;
V – do RPON-PRODAM;
VI – do Programa de Integridade e Boas Práticas (PIBP) da PRODAM;
VII – das Políticas Internas de Integridade, Ética, Segurança da Informação e Compliance da PRODAM.

7.1.2. As PARCEIRAS comprometem-se a manter, durante toda a vigência deste Contrato, ambiente íntegro, seguro, rastreável e livre de práticas ilícitas, observado o papel institucional da PRODAM como empresa pública municipal.

7.2 – Obrigações da PARCEIRA em Matéria de Compliance e Integridade.

7.2.1. A PARCEIRA deverá manter Programa de Integridade, proporcional ao seu porte e risco, contendo, no mínimo:

a) código de ética e conduta;
b) controles internos antifraude;

c) mecanismos de combate ao suborno, corrupção e vantagem indevida;
d) políticas de relacionamento com agentes públicos;
e) processos de denúncia e canais de integridade;
f) mecanismos de prevenção à lavagem de dinheiro e ao financiamento ao terrorismo;
g) políticas de governança de tecnologia e proteção de dados;
h) treinamentos periódicos obrigatórios a seus empregados.

7.2.2. A PARCEIRA declara que não está impedida, por ação judicial, administrativa ou regulatória, de contratar com o poder público.

7.2.3. A PARCEIRA declara ainda que não foi condenada, nos últimos 5 anos, por:

a) corrupção;
b) fraude contra a administração pública;
c) atos lesivos previstos na Lei nº 12.846/2013;
d) concorrência desleal;
e) práticas anticompetitivas.

7.2.4. A PARCEIRA deverá comunicar à PRODAM, imediatamente, qualquer investigação, sanção, processo ou procedimento que possa afetar sua reputação, integridade ou capacidade de execução do SMARTSAMPA.

7.3 – Due Diligence Inicial e Contínua:

7.3.1. A PARCEIRA sujeita-se à realização de Due Diligence de Integridade inicial, como condição para assinatura deste Contrato, abrangendo:

I – análise reputacional;
II – verificação de antecedentes;
III – revisão de governança e compliance;
IV – análise de riscos de corrupção e vínculo com agentes públicos;
V – verificação de capacidade técnica e operacional;
VI – consulta a bases públicas e privadas;
VII – avaliação de riscos prevista no RPON-PRODAM.

7.3.2. A PARCEIRA compromete-se a cooperar integralmente com a Due Diligence, fornecendo documentos, informações e evidências quando solicitados.

7.3.3. A PRODAM poderá realizar Due Diligence Contínua ao longo da vigência da parceria, sempre que necessário para:

I – mitigar riscos;
II – avaliar incidentes;
III – revalidar a integridade;
IV – adequar-se a mudanças relevantes no controle societário da PARCEIRA.

7.4 – Prevenção de Conflitos de Interesse:

7.4.1. As PARCEIRAS deverão adotar medidas preventivas contra conflitos de interesse reais, potenciais ou aparentes, inclusive:

I – restrição a participação de agentes públicos em atividades que possam influenciar decisões da PARCEIRA;
II – proibição de atos que possam beneficiar indevidamente pessoas físicas vinculadas às PARCEIRAS;
III – segregação de funções entre planejamento, execução, validação e fiscalização;
IV – comunicação imediata de situações de conflito identificadas.

7.4.2. A ocorrência de conflito de interesse não comunicado constitui infração grave a este Contrato.

7.5 – Conduta Ética e Proibições Explicitas

7.5.1. É vedado às PARCEIRAS, direta ou indiretamente:

I – oferecer, prometer, solicitar ou aceitar vantagem indevida;
II – financiar atos ilícitos ou anticompetitivos;
III – praticar fraude, conluio ou manipular etapas do processo decisório;
IV – utilizar informações sigilosas para benefício próprio ou de terceiros;
V – influenciar decisões administrativas por meios ilícitos ou antiéticos;
VI – contratar ou subcontratar empresas impedidas, inidôneas ou sancionadas.

7.5.2. Toda suspeita, denúncia ou evidência de irregularidade deverá ser:

a) tratada com absoluta confidencialidade;
b) encaminhada ao canal de integridade da PRODAM;
c) registrada no processo administrativo da ON;
d) objeto de investigação adequada.

7.6 – Auditorias, Verificação Independente e Acesso a Informações

7.6.1. A PARCEIRA admite auditorias:

I – da PRODAM;
II – da Controladoria Geral do Município;
III – do Tribunal de Contas do Município;
IV – do Ministério Público;
V – de órgãos de controle interno e externo;
VI – de auditorias independentes determinadas pela PRODAM.

7.6.2. A PARCEIRA deverá fornecer, tempestivamente, todos os documentos e informações solicitados.

7.6.3. A recusa injustificada à auditoria constitui descumprimento contratual grave.

7.7 – Consequências de Violação

7.7.1. A violação às normas de integridade, compliance ou anticorrupção poderá resultar em:

I – suspensão das atividades;
II – afastamento de membros da equipe;
III – plano de ação obrigatória;
IV – notificação formal no processo;
V – rescisão unilateral por justa causa;
VI – comunicação às autoridades competentes;
VII – aplicação de sanções civis, administrativas e criminais.

7.8 – Declarações de Integridade

7.8.1. As PARCEIRAS declaram que:

I – cumprem todas as leis aplicáveis;
II – não mantêm práticas que violem integridade ou anticorrupção;
III – manterão registros contábeis transparentes;
IV – adotarão políticas internas compatíveis com este Contrato;
V – não utilizarão a parceria para fins ilícitos.

CLÁUSULA 8 – PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

8.1 – Princípios Gerais de Tratamento de Dados

8.1.1. Todo e qualquer tratamento de dados pessoais, dados pessoais sensíveis, dados cadastrais, dados territoriais, dados de mobilidade, bases georreferenciadas e demais informações manipuladas no contexto da Oportunidade de Negócio SMARTSAMPA deverá observar, rigorosamente:

I – a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);
II – a legislação municipal aplicável;
III – o Regulamento de Parcerias em Oportunidades de Negócio – RPON-PRODAM;
IV – as Políticas de Segurança da Informação, Cibersegurança, Governança de Dados e Interoperabilidade da PRODAM-SP;
V – as regras estabelecidas nos Anexo A – Tratamento de Dados Pessoais, parte integrante deste Contrato e do Anexo E – Relatório de Impacto de Proteção de Dados.

8.1.2. O tratamento de dados pessoais deverá sempre respeitar:

a) finalidade legítima e específica;
b) necessidade e minimização;
c) adequação;
d) segurança;
e) prevenção;
f) transparência nos limites da lei;
g) responsabilização e prestação de contas;
h) direitos dos titulares previstos no art. 18 da LGPD.

8.2 – Papéis das PARCEIRAS no Tratamento de Dados (LGPD)

8.2.1. Para fins de tratamento de dados pessoais no âmbito do SMARTSAMPA, as PARCEIRAS poderão assumir, conforme o caso e a situação de uso:

I – a condição de Controladora;
II – a condição de Operadora;
III – a condição de Controladoras Conjuntas, conforme definido em ato específico da governança da ON.

8.2.2. A definição dos papéis será detalhada no Anexo A – Tratamento de Dados Pessoais, podendo ser revista pela governança da ON conforme evolução da solução.

8.2.3. A PARCEIRA não poderá tratar dados pessoais para finalidades diversas das previstas neste Contrato, no PNO ou em normas aplicáveis.

8.3 – Bases de Dados Municipais

8.3.1. O acesso a bases públicas municipais, incluindo dados cadastrais, dados territoriais, dados geoespaciais, dados de mobilidade, logs, cadastros técnicos, bases de sensores IoT, APIs internas e externas, somente poderá ocorrer mediante autorização formal da PRODAM e exclusivamente para fins da execução da Oportunidade de Negócio SMARTSAMPA.

8.3.2. A PARCEIRA reconhece que tais bases possuem caráter institucional e estratégico, sendo proibida sua utilização para:

I – benefício próprio ou de terceiros;
II – fins comerciais externos à ON;
III – treinamentos indevidos de IA;
IV – qualquer finalidade diversa da execução deste Contrato.

8.4 – Segurança da Informação e Cibersegurança

8.4.1. As PARCEIRAS deverão adotar medidas técnicas e administrativas de segurança

compatíveis com o risco do tratamento, observando:

I – políticas internas da PRODAM;
II – padrões internacionais de cibersegurança (como ISO 27001, ISO 27701, NIST, quando aplicáveis);
III – diretrizes municipais de segurança da informação;
IV – requisitos definidos no PNO.

8.4.2. Dentre as medidas mínimas obrigatórias estão:

a) criptografia de dados em trânsito e em repouso;
b) controles de acesso baseados em perfil e necessidade;
c) autenticação forte e múltiplo fator;
d) logs imutáveis e rastreáveis;
e) segregação de ambientes;
f) backups periódicos;
g) monitoramento contínuo de ameaças;
h) proteção contra malware, exploits, ransomware e ataques de negação de serviço (DDoS);
i) auditoria de código-fonte (quando aplicável).

8.5 – Incidentes de Segurança e Comunicação Imediata

8.5.1. Qualquer incidente de segurança ou suspeita de violação envolvendo dados pessoais, dados territoriais, bases municipais ou informações sigilosas deverá ser comunicado imediatamente à PRODAM, no prazo máximo de:

até 2 (duas) horas após ciência, no caso de incidentes críticos;

até 24 (vinte e quatro) horas nos demais incidentes relevantes.

8.5.2. A PARCEIRA deverá fornecer informações que permitam à PRODAM:

I – avaliar o impacto;
II – acionar protocolos de resposta a incidentes;
III – comunicar autoridades competentes, se necessário (CGM, ANPD etc.);
IV – adotar medidas de mitigação.

8.5.3. A PARCEIRA deverá cooperar integralmente com eventuais investigações.

8.6 – Confidencialidade de Dados e Informações Sensíveis

8.6.1. Os dados tratados no âmbito do SMARTSAMPA são considerados, salvo legislação aplicável, informações protegidas, sujeitas ao regime de sigilo do Anexo D e às normas internas de classificação da PRODAM.

8.6.2. A divulgação só será permitida:

I – mediante autorização expressa;
II – por decisão judicial;
III – por determinação legal;
IV – nos limites do dever de transparência da administração pública, observado o sigilo de dados pessoais.

8.7 – Acesso a Sistemas e Auditoria Técnica

8.7.1. O acesso da PARCEIRA aos ambientes, sistemas, APIs, logs, bancos de dados e estruturas da PRODAM dependerá de credenciais formais e individuais.

8.7.2. A PRODAM poderá auditar:

I – acessos;
II – logs;
III – integrações;
IV – funcionalidades;
V – mecanismos de segurança;
VI – fluxos de dados pessoais.

8.7.3. A recusa à auditoria ou a tentativa de ocultação de informação ensejará medidas corretivas, inclusive rescisão.

8.8 – Processamento e Armazenamento de Dados

8.8.1. Os dados tratados no âmbito do SMARTSAMPA deverão ser armazenados:

I – em ambiente autorizado pela PRODAM;
II – preferencialmente em infraestrutura pública municipal ou soluções acordadas no PNO;
III – com redundância e proteção contra perda, corrupção ou acesso não autorizado.

8.8.2. A PARCEIRA não poderá armazenar dados municipais fora dos ambientes definidos pela PRODAM, salvo autorização expressa e documentada.

8.9 – Direitos dos Titulares

8.9.1. As PARCEIRAS deverão assegurar os direitos dos titulares previstos no art. 18 da LGPD.

8.9.2. Quando a PARCEIRA receber requisição de titular, deverá:

a) registrar internamente;
b) comunicar à PRODAM em até 48h;
c) aguardar orientação, quando o tratamento envolver dados municipais.

8.10 – Eliminação, Devolução ou Anonimização

8.10.1. Ao término deste Contrato, ou quando determinado pela PRODAM, a PARCEIRA deverá:

I – eliminar ou anonimizar dados pessoais;
II – devolver dados territoriais, cadastrais ou bases que pertençam ao Município;
III – apresentar relatório de eliminação;
IV – garantir a destruição segura de mídias e suportes.

8.11 – Responsabilidade por Violação

8.11.1. A PARCEIRA responderá integralmente por danos causados por:

I – violação de dados pessoais;
II – incidente de segurança por falha sua;
III – uso indevido de dados municipais;
IV – descumprimento da LGPD;
V – falha dos seus colaboradores, prepostos ou subcontratados.

8.11.2. A PRODAM responderá na medida de sua responsabilidade, conforme o papel que exercer no tratamento.

CLÁUSULA 9 – PROPRIEDADE INTELECTUAL

9.1 – Princípios Gerais

9.1.1. A propriedade intelectual, os direitos autorais, os direitos sobre softwares, algoritmos, bancos de dados, modelos de IA, designs, interfaces, marcas, patentes e demais ativos intangíveis relacionados à Oportunidade de Negócio SMARTSAMPA observarão:

I – a legislação brasileira aplicável (Lei nº 9.279/1996; Lei nº 9.609/1998; Lei nº 9.610/1998; Código Civil; LGPD);
II – o RPON-PRODAM, especialmente suas regras sobre propriedade intelectual derivada de parcerias;
III – as políticas internas de segurança, inovação e governança da PRODAM;
IV – o PNO e seus anexos, que especificam a natureza dos ativos tecnológicos e sua composição.

9.2 – Licenciamento entre as Partes

9.3.1. A PARCEIRA concede à PRODAM, de forma gratuita, irrevogável e não exclusiva, licença para:

I – usar, executar, integrar e testar seus ativos preexistentes, na medida necessária à operação

do SMARTSAMPA;
II – desenvolver, internamente ou por terceiros, melhorias, patches, correções, integrações ou adaptações de compatibilidade;
III – manter a continuidade do serviço em caso de interrupção ou descontinuidade da PARCEIRA.

9.4 – Direitos sobre Software e Código-Fonte

9.4.1. Os softwares desenvolvidos no âmbito da ON serão classificados como:

a) propriedade conjunta (quando decorrentes de desenvolvimento colaborativo);
b) propriedade exclusiva de uma das PARCEIRAS (nos termos dos itens anteriores);
c) licença de uso (quando pertencentes exclusivamente a uma das PARCEIRAS).

9.4.2. O código-fonte dos ativos conjuntos deve ser:

I – versionado;
II – documentado;
III – armazenado em repositório seguro;
IV – com controle de acesso gerenciado pela PRODAM.

9.4.3. O acesso ao código-fonte de ativos exclusivos da PARCEIRA poderá ocorrer somente para:

I – fins de auditoria;
II – fins de segurança e continuidade;
III – situações de incidentes críticos.

9.5 – Marcas, Nome “SMARTSAMPA” e Identidade Visual

9.5.1. A marca SMARTSAMPA, seus logotipos, identidade visual, domínios, denominações e elementos correlatos são de:

I – titularidade exclusiva da PRODAM;
II – e sua utilização pela PARCEIRA dependerá de autorização expressa e formal.

9.5.2. Qualquer pedido de registro de marca relacionado ao sistema da solução deverá ser submetido à PRODAM.

9.6 – Uso da Propriedade Intelectual fora do Escopo da ON

9.6.1. É vedado à PARCEIRA:

I – usar ativos conjuntos para fins comerciais externos;
II – sublicenciar, vender ou disponibilizar a terceiros ativos conjuntos;
III – desenvolver produtos concorrentes utilizando ativos da ON;

IV – explorar dados municipais ou algoritmos da solução para finalidades estranhas ao contrato.

9.6.2. A exploração de ativos conjuntos fora do escopo da ON dependerá de:

a) validação da governança da ON;
b) autorização formal da PRODAM;
c) repartição de resultados, quando aplicável.

9.7 – Segredos Empresariais e Confidencialidade Técnica

9.7.1. As PARCEIRAS se comprometem a proteger:

I – código-fonte;
II – algoritmos;
III – métodos de inferência;
IV – modelos de IA;
V – frameworks, bibliotecas e estruturas internas;
VI – documentação técnica;
VII – protocolos proprietários.

9.7.2. O uso desses elementos é limitado exclusivamente ao desenvolvimento e execução do SMARTSAMPA.

9.8 – Regime de Copropriedade

9.8.1. Na hipótese de propriedade conjunta, aplicam-se os seguintes princípios:

I – ambas as PARCEIRAS poderão usar os ativos conjuntos dentro da ON sem limitação;
II – exploração externa dependerá da governança da ON e de acordo específico;
III – cada PARCEIRA poderá registrar a copropriedade no INPI;
IV – disputas serão resolvidas por governança conjunta.

9.8.2. Quaisquer melhorias realizadas sobre ativos conjuntos serão automaticamente incorporadas à copropriedade.

9.9 – Descontinuidade, Continuidade Operacional e Transferência Técnica

9.9.1. Em caso de rescisão, a PARCEIRA deverá:

I – transferir para a PRODAM todo ativo conjunto;
II – entregar documentação completa;
III – fornecer suporte técnico para transição por até 90 dias;
IV – permitir à PRODAM desenvolver ou contratar terceiros para continuidade.

9.9.2. A PRODAM poderá manter a operação normal da solução, sem limitação.

9.10 – Responsabilidade por Violação de Direitos Autorais ou PI de Terceiros

9.10.1. A PARCEIRA será responsável por quaisquer violações a direitos autorais, propriedade intelectual ou patentes de terceiros decorrentes de:

I – código próprio;
II – integrações desenvolvidas por ela;
III – bibliotecas incluídas indevidamente;
IV – modelos proprietários de IA utilizados irregularmente.

9.10.2. A PARCEIRA deverá indenizar a PRODAM por eventuais prejuízos, inclusive judiciais.

CLÁUSULA 10 – DOS VALORES, APORTES, CUSTOS E CRITÉRIOS FINANCEIROS

10.1 – Natureza não remuneratória da relação

10.1.1. As PARCEIRAS reconhecem que o presente Contrato possui natureza estritamente associativa, não estabelecendo relação de fornecimento de bens, prestação de serviços, terceirização ou qualquer forma de contratação remuneratória entre as partes.

10.1.2. Não haverá, entre as PARCEIRAS:

I – pagamento de preço;
II – cobrança por serviços;
III – faturamento mínimo ou garantido;
IV – repasses unilaterais;
V – remuneração direta ou indireta por atividades executadas.

10.2 – Aportes, recursos e investimentos

10.2.1. Cada PARCEIRA será responsável pelos aportes, investimentos, recursos materiais, humanos, tecnológicos e financeiros necessários ao cumprimento das obrigações que lhe forem atribuídas neste Contrato, no PNO e na Matriz de Riscos.

10.2.2. Os aportes poderão incluir, sem limitação:

a) alocação de equipe;
b) disponibilização de infraestrutura;
c) uso de ativos tecnológicos preexistentes;
d) aquisição ou contratação de recursos complementares;
e) disponibilização de ambientes de teste, homologação e produção;
f) investimentos para evolução da solução.

10.2.3. A proporcionalidade dos aportes constará no PNO, podendo ser revista pela governança da ON.

10.3 – Custos diretos, despesas operacionais e rateios

10.3.1. As PARCEIRAS poderão assumir custos diretos vinculados à execução da ON, observadas as alocações definidas no PNO.

10.3.2. Poderão ser objeto de compartilhamento ou rateio:

I – despesas com infraestrutura tecnológica;
II – custos de ambientes, conectividade, redes, certificações e segurança;
III – despesas com APIs, integrações e licenças necessárias ao funcionamento da solução;
IV – investimentos para ampliação da capacidade;
V – despesas de suporte, documentação, testes e auditorias técnicas.

10.3.3. Eventuais rateios de custos deverão atender cumulativamente:

a) proporcionalidade dos aportes;
b) matriz de riscos;
c) autorização do Comitê de Governança;
d) registro formal no processo administrativo da ON.

10.4 – Custos extraordinários

10.4.1. Despesas extraordinárias, não previstas originalmente no PNO, somente poderão ser realizadas:

I – mediante justificativa técnica;
II – com aprovação do Comitê de Governança;
III – com atualização da Matriz de Riscos;
IV – sem implicar contraprestação entre as PARCEIRAS.

10.5 – Contabilização, transparência e auditoria financeira

10.5.1. Cada PARCEIRA deverá manter a rastreabilidade dos gastos, investimentos, despesas e custos incorridos no âmbito da ON, de forma:

a) segregada;
b) documentada;
c) auditável;
d) compatível com normas contábeis aplicáveis;
e) disponível aos órgãos de controle interno e externo.

10.5.2. A PARCEIRA deverá disponibilizar, quando solicitado pela PRODAM:

I – demonstrativos de custos;
II – planilhas de alocação de recursos;
III – notas explicativas sobre aportes;
IV – documentos comprobatórios de despesas elegíveis.

10.5.3. A recusa injustificada em fornecer tais informações configura infração grave.

10.6 – Ausência de solidariedade financeira

10.6.1. Cada PARCEIRA será exclusivamente responsável por suas obrigações financeiras, fiscais, trabalhistas e operacionais decorrentes dos aportes e investimentos próprios.

10.6.2. A execução deste Contrato não implica:

I – solidariedade;
II – garantia;
III – coobrigação;
IV – assunção de dívidas de outra PARCEIRA.

10.7 – Relação com a próxima cláusula (Exploração Econômica)

10.7.1. A presente cláusula regula apenas valores internos, aportes e custos entre as PARCEIRAS.

10.7.2. A receita, monetização e exploração do SMARTSAMPA perante clientes externos será disciplinada na Cláusula de Exploração Econômica e Compartilhamento de Resultados, respeitando:

I – proporcionalidade contributiva;
II – Matriz de Riscos;
III – modelo econômico definido no PNO;
IV – governança da ON.

CLÁUSULA 11 – EXPLORAÇÃO ECONÔMICA E COMPARTILHAMENTO DE RESULTADOS

11.1. A exploração econômica da Oportunidade de Negócio SMARTSAMPA será realizada de forma conjunta pelas PARCEIRAS, observando:

I – o caráter associativo deste Contrato;
II – o modelo de negócios definido no PNO;
III – a Matriz de Riscos;
IV – as deliberações da governança da ON;
V – os princípios da Lei nº 13.303/2016;

VI – os objetivos de inovação e transformação urbana da solução.

11.1.1. As PARCEIRAS reconhecem que a geração de receita dependerá das contratações realizadas com Clientes externos, públicos ou privados, não havendo garantia de demanda ou faturamento mínimo.

11.2 – Modalidades de Exploração Econômica

11.2.1. O SMARTSAMPA poderá ser comercializado ou disponibilizado a terceiros por meio de, entre outros:

I – licenciamento de uso;
II – disponibilização de SaaS (software as a service);
III – implantação de módulos ou componentes;
IV – comercialização de serviços acessórios ou integrados;
V – prestação de apoio técnico de evolução;
VI – uso de APIs, dados analíticos e integrações, quando permitido;
VII – assinaturas, pacotes, planos ou modelos híbridos.

11.2.2. A definição dos modelos e submodelos de monetização será feita pela governança da ON, respeitando o PNO.

11.3 – Precificação e Política Comercial

11.3.1. Os preços, valores de licenciamento, assinaturas, modelos de contratação, descontos e condições comerciais serão estabelecidos:

I – pela PRODAM, como agente público e líder institucional da ON;
II – com base em estudos de mercado;
III – considerando a estratégia comercial definida no PNO;
IV – com parecer técnico e jurídico quando necessário;
V – com validação do Comitê de Governança.

11.3.2. A PARCEIRA poderá propor ajustes de precificação, devendo apresentar fundamentação técnica e de mercado.

11.4 – Receitas elegíveis para compartilhamento

11.4.1. São elegíveis ao compartilhamento entre as PARCEIRAS todas as receitas decorrentes da exploração externa da solução, incluindo:

I – licenças de uso;
II – valor de módulos, funcionalidades e integrações;
III – assinaturas e planos recorrentes;
IV – serviços acessórios previstos no modelo de negócios;

V – valores obtidos com customizações ou extensões;
VI – monetização de dados analíticos autorizados e legalmente admitidos;
VII – receitas oriundas de expansão para novos clientes, territórios ou setores.

11.4.2. Não são elegíveis ao compartilhamento:

I – receitas decorrentes de produtos exclusivos da PRODAM ou da PARCEIRA não relacionados;
II – receitas geradas por ativos preexistentes utilizados isoladamente;
III – receitas originadas de serviços não previstos no escopo da ON.

11.5 – Critério de Rateio das Receitas

11.5.1. O rateio das receitas será definido no PNO, considerando:

I – proporcionalidade dos aportes realizados (técnicos, financeiros, humanos e tecnológicos);
II – riscos assumidos por cada PARCEIRA;
III – custos diretos e indiretos necessários à operação;
IV – contribuições técnicas e estratégicas;
V – participação na propriedade intelectual conjunta;
VI – governança e responsabilidades específicas.

11.5.2. O rateio poderá adotar modelos como:

a) percentual fixo pré-estabelecido;
b) percentual variável conforme tipo de cliente;
c) repartição por módulo, componente ou camada;
d) critérios híbridos ou escalonados.

11.5.3. O rateio deverá ser:

I – objetivo;
II – auditável;
III – registrado no processo administrativo;
IV – aprovado pela governança da ON.

11.6 – Custos, Despesas e Tributos Relacionados à Comercialização

11.6.1. Antes do compartilhamento de resultados, poderão ser descontados:

I – tributos incidentes;
II – custos diretos de comercialização;
III – despesas operacionais elegíveis;
IV – custos extraordinários autorizados pelo Comitê de Governança.

11.6.2. Não serão deduzidos custos ou despesas:

I – não previstas no PNO;
II – que caracterizem prestação de serviços entre as PARCEIRAS;
III – vinculadas a produtos externos à ON.

11.7 – Inadimplência, Cancelamento e Reversões

11.7.1. Em caso de inadimplência de clientes, a governança da ON deverá:

I – avaliar impacto econômico;
II – decidir sobre cobrança administrativa;
III – definir eventual rateio de risco, conforme Matriz de Riscos;
IV – revisar modelos de garantia, quando aplicáveis.

11.7.2. Valores estornados ou cancelados serão ajustados no rateio subsequente.

11.8 – Relatórios Econômicos e Prestação de Contas

11.8.1. A PRODAM deverá manter:

I – registro contábil separado das receitas;
II – relatório trimestral de exploração;
III – painéis financeiros e indicadores econômicos;
IV – evidências das receitas obtidas.

11.8.2. A PARCEIRA terá acesso aos demonstrativos financeiros, observadas as regras de confidencialidade.

11.9 – Auditoria Econômica

11.9.1. A PRODAM poderá realizar auditorias periódicas para verificar:

I – correção das receitas apresentadas;
II – critérios de rateio;
III – comprovação de custos elegíveis;
IV – conformidade com o PNO.

11.9.2. A PARCEIRA deverá cooperar integralmente.

11.10 – Ausência de Exclusividade

11.10.1. Salvo disposição expressa em contrário, a PARCEIRA reconhece que a PRODAM poderá:

I – comercializar o SMARTSAMPA diretamente;

II – celebrar contratos com múltiplos clientes;
III – firmar parcerias complementares, desde que não haja conflito de interesse.

11.11 – Revisão do Modelo Econômico

11.11.1. O modelo econômico poderá ser revisado quando:

I – houver mudanças no mercado;
II – ocorrer evolução tecnológica significativa;
III – surgirem novos módulos ou ecossistemas;
IV – houver alteração regulatória;
V – a governança assim deliberar.

11.12 – Irretratabilidade das Receitas já Rateadas

11.12.1. As receitas compartilhadas são definitivas, não sendo passíveis de reversão, exceto em caso de:

I – fraude comprovada;
II – erro material;
III – determinação judicial.

CLÁUSULA 12 – CONFIDENCIALIDADE E INFORMAÇÕES SIGILOSAS
/
12.1 – Definição de Informações Sigilosas

12.1.1. Para fins deste Contrato, consideram-se Informações Sigilosas todas as informações, dados, documentos, estratégias, artefatos, especificações técnicas, códigos, algoritmos, arquiteturas, fluxos, integrações, APIs, modelos de negócio, bases territoriais, dados pessoais, informações cadastrais, comerciais, institucionais, tecnológicas ou operacionais, em qualquer formato ou suporte, que:

I – sejam classificadas como sigilosas pela PRODAM ou pela governança da ON;
II – sejam protegidas por segredo legal, fiscal, administrativo ou contratual;
III – envolvam segurança pública, segurança da informação ou infraestrutura crítica;
IV – se relacionem à arquitetura interna do SMARTSAMPA e seus módulos;
V – se refiram a dados pessoais ou sensíveis regidos pela LGPD;
VI – tenham sido obtidas em decorrência da execução deste Contrato.

12.1.2. Consideram-se também sigilosas:

a) logs, registros de auditoria, relatórios e análises internas;
b) documentação interna de sistemas municipais;
c) informações de clientes, potenciais clientes e parceiros;
d) cenários de risco, avaliações de integridade e due diligence;

e) dados de mobilidade, eventos urbanos e bases territoriais.

12.2 – Obrigações de Confidencialidade

12.2.1. As PARCEIRAS comprometem-se a:

I – manter absoluto sigilo sobre todas as Informações Sigilosas;
II – usar as informações exclusivamente para execução deste Contrato;
III – impedir o acesso de terceiros não autorizados;
IV – adotar medidas técnicas e administrativas compatíveis com seu grau de sensibilidade;
V – comunicar imediatamente qualquer incidente, violação ou suspeita de acesso indevido.

12.2.2. A confidencialidade abrange, sem limitação:

a) apresentações internas;
b) gravações, prints, documentos, e-mails e comunicações técnicas;
c) relatórios, códigos, scripts, versões e diagramas;
d) conhecimento técnico adquirido no contexto da ON;
e) materiais do PNPO, PNO, Matriz de Riscos, governança e roadmap.

12.3 – Acesso Restrito e Princípio do “Need to Know”

12.3.1. O acesso às Informações Sigilosas será limitado apenas aos colaboradores, empregados, prepostos e representantes que:

I – necessitem das informações para cumprir obrigações deste Contrato;
II – tenham sido formalmente autorizados pela PARCEIRA responsável;
III – estejam submetidos a obrigações de sigilo equivalentes.

12.3.2. As PARCEIRAS devem manter registros claros dos acessos concedidos.

12.4 – Exceções à Confidencialidade

12.4.1. O dever de sigilo não se aplica às informações que:

I – se tornarem públicas sem violação deste Contrato;
II – forem comprovadamente de conhecimento prévio da PARCEIRA receptora;
III – forem desenvolvidas independentemente pela PARCEIRA receptora;
IV – forem legitimamente recebidas de terceiros sem violação de sigilo;
V – devam ser divulgadas por determinação legal, regulatória ou judicial.

12.4.2. Em caso de obrigação legal de divulgação, a PARCEIRA deverá:

a) comunicar previamente a outra PARCEIRA, quando possível;
b) limitar a divulgação ao mínimo necessário;

c) assegurar que a informação receba o tratamento legal adequado.

12.5 – Gestão de Classificação da Informação

12.5.1. As Informações Sigilosas serão classificadas conforme política interna da PRODAM.

12.5.2. Caberá à PRODAM a classificação de dados municipais, territoriais, cadastrais, georreferenciados ou relacionados à infraestrutura crítica da cidade.

12.5.3. A PARCEIRA deverá seguir rigorosamente as normas de classificação, proteção, armazenamento, cópia, transporte e descarte seguro de informações.

12.6 – Proibição de Uso Indevido

12.6.1. É expressamente vedado às PARCEIRAS:

I – usar Informações Sigilosas para fins próprios, externos ou comerciais não relacionados à ON;
II – desenvolver soluções, produtos ou serviços concorrentes utilizando ativos sigilosos;
III – utilizar dados municipais para treinamento de modelos de IA sem autorização expressa;
IV – explorar bases municipais para finalidade diversa da execução do contrato;
V – compartilhar informações com terceiros sem autorização documentada.

12.6.2. A violação desta cláusula constitui infração grave, podendo ensejar:

a) rescisão imediata;
b) indenização integral pelos danos causados;
c) comunicação às autoridades competentes;
d) bloqueio de acessos e retirada da equipe envolvida.

12.7 – Duração do Dever de Confidencialidade

12.7.1. O dever de sigilo:

I – terá início na data de assinatura deste Contrato;
II – permanecerá vigente durante toda a sua execução;
III – subsistirá **por 10 (dez) anos** após o término ou rescisão, salvo:
a) quando envolver dados pessoais (prazo ilimitado enquanto houver obrigação legal);
b) quando envolver segredo industrial da PRODAM (prazo indefinido).

12.8 – Devolução e Descarte de Informações

12.8.1. Ao término da ON, ou mediante solicitação da PRODAM, a PARCEIRA deverá:

I – devolver todos os documentos, ativos e registros sigilosos;
II – destruir cópias e mídias que contenham tais informações;

III – apresentar relatório formal de descarte seguro;
IV – manter registros de eliminação conforme normas da PRODAM.

12.9 – Violação, Incidentes e Responsabilidades

12.9.1. A violação de confidencialidade sujeitará a parte infratora:

I – à reparação integral dos danos;
II – às penalidades previstas no contrato;
III – à eventual responsabilização administrativa, civil e criminal;
IV – ao afastamento da equipe envolvida;
V – à possível rescisão do contrato.

12.9.2. Incidentes deverão ser tratados conforme:

I – protocolos do Comitê de Segurança da Informação da PRODAM;
II – LGPD e suas orientações de mitigação;
III – Matriz de Riscos da ON;
IV – Cláusula de Proteção de Dados deste Contrato.

CLÁUSULA 13 – DA EXCLUSIVIDADE, NÃO CONCORRÊNCIA E PREVENÇÃO DE CONFLITO DE INTERESSES

13.1. Natureza e finalidade da cláusula

13.1.1. As PARCEIRAS reconhecem que o presente Contrato possui natureza estritamente associativa, estratégica e inovadora, envolvendo o compartilhamento de informações sensíveis, ativos tecnológicos, conhecimentos técnicos, estratégias comerciais e modelos de negócio que constituem vantagem competitiva relevante da Oportunidade de Negócio SMARTSAMPA.

3.1.2. Em razão dessa natureza, a presente cláusula tem por finalidade preservar a integridade econômica, técnica e estratégica da parceria, prevenindo situações de concorrência desleal, conflito de interesses, canibalização do modelo de negócio e exposição indevida de informações ou ativos estratégicos.

13.2. Vedação à atuação concorrencial da PARCEIRA

13.2.1. Durante a vigência deste Contrato, a PARCEIRA obriga-se a não desenvolver, explorar, licenciar, comercializar, operar ou apoiar, direta ou indiretamente, por si ou por intermédio de terceiros, solução, produto, serviço ou plataforma que seja:

I – idêntica, equivalente ou funcionalmente substituível, no todo ou em parte relevante, à solução SMARTSAMPA ou a seus módulos, componentes, integrações ou funcionalidades estratégicas; ou

II – destinada ao mesmo mercado-alvo, público ou privado, quando tal atuação puder comprometer a exploração econômica, a diferenciação competitiva ou o posicionamento estratégico da Oportunidade de Negócio SMARTSAMPA.

13.3. Relações com terceiros e conflitos concorrenciais

13.3.1. A PARCEIRA compromete-se a não manter, firmar ou ampliar, durante a vigência deste Contrato, relações contratuais, societárias, comerciais, tecnológicas ou estratégicas com terceiros que atuem como concorrentes diretos da solução SMARTSAMPA, quando tais relações puderem:

I – permitir compartilhamento, ainda que indireto, de informações sigilosas, técnicas, comerciais ou estratégicas;
II – viabilizar replicação, espelhamento ou reaproveitamento do modelo de negócio;
III – reduzir ou neutralizar o diferencial competitivo da Oportunidade de Negócio.

13.3.2. Incluem-se na vedação prevista no item anterior as hipóteses de:

I – participação societária relevante, direta ou indireta;
II – acordos de licenciamento, sublicenciamento ou cooperação tecnológica;
III – fornecimento da mesma solução ou solução equivalente a terceiros concorrentes;
IV – atuação como integradora, revendedora, operadora ou parceira estratégica de soluções concorrentes.

13.4. Conceito de conflito concorrencial

13.4.1. Para fins deste Contrato, considera-se conflito concorrencial toda situação real, potencial ou aparente que possa:

I – comprometer a confiança, a lealdade e a boa-fé objetiva entre as PARCEIRAS;
II – expor ativos estratégicos, informações sensíveis ou segredos de negócio;
III – afetar negativamente a viabilidade econômica, técnica ou estratégica da Oportunidade de Negócio SMARTSAMPA.

3.5. Dever de informação e mitigação

13.5.1. A PARCEIRA deverá comunicar imediatamente à PRODAM, por escrito e de forma circunstanciada, qualquer situação superveniente que possa caracterizar conflito concorrencial nos termos desta cláusula.

13.5.2. A PRODAM poderá, a seu exclusivo critério:

I – exigir medidas de mitigação de risco;
II – impor restrições operacionais específicas;
III – determinar ajustes na governança da parceria; ou

IV – declarar a incompatibilidade da situação com a manutenção da parceria.

13.6. Consequências do descumprimento

13.6.1. O descumprimento de qualquer disposição desta cláusula caracteriza infração contratual grave, ensejando, isolada ou cumulativamente:

I – rescisão imediata deste Contrato, por justa causa;
II – perda do direito de exploração econômica conjunta;
III – indenização integral pelos danos diretos e indiretos causados à PRODAM;
IV – adoção das medidas administrativas, civis e judiciais cabíveis.

13.7. Sobrevivência da obrigação

13.7.1. As obrigações previstas nesta cláusula subsistirão pelo prazo **de 5 (cinco) anos** após o término ou rescisão deste Contrato, no que couber à proteção de informações, ativos, estratégias e vantagens competitivas decorrentes da parceria.

CLÁUSULA 14 – MATRIZ DE RISCOS E GESTÃO DE RISCOS

14.1 – Função da Matriz de Riscos

14.1.1. A Matriz de Riscos da Oportunidade de Negócio SMARTSAMPA, constante do PNO e incorporada a este Contrato como Anexo C, estabelece:

I – a identificação dos riscos inerentes à ON;
II – sua classificação, impacto e probabilidade;
III – a alocação de responsabilidades entre as PARCEIRAS;
IV – medidas preventivas, mitigadoras e corretivas;
V – mecanismos de monitoramento e governança.

14.1.2. A Matriz de Riscos constitui documento vinculante, prevalecendo sobre interpretações subjetivas e suplementando as obrigações deste Contrato.

14.2 – Princípios da Gestão de Riscos

A gestão de riscos da ON observará:

I – prevenção;
II – proporcionalidade;
III – transparência e rastreabilidade das decisões;
IV – cooperação técnica entre as PARCEIRAS;
V – mitigação contínua;
VI – segregação de funções;

VII – aderência às políticas internas da PRODAM;
VIII – aderência aos padrões de governança pública aplicáveis.

14.3 – Classificação dos Riscos

Os riscos da ON serão agrupados, no mínimo, nas seguintes categorias:

I – Riscos Tecnológicos

a) indisponibilidade de sistemas;
b) falhas de APIs, integrações, módulos ou arquitetura;
c) bugs, vulnerabilidades, exploits e falhas de desempenho;
d) obsolescência tecnológica;
e) erros de implantação ou atualização.

II – Riscos de Segurança da Informação e Cibernéticos

a) ataques cibernéticos;
b) acesso indevido a dados municipais;
c) quebra de sigilo ou vazamento;
d) interceptação de tráfego ou intrusão;
e) comprometimento de credenciais.

III – Riscos de Dados

a) violação de dados pessoais;
b) uso indevido de dados territoriais e cadastrais;
c) inconsistências, duplicidades ou corrupção de dados;
d) falhas em bases ou fluxos críticos do Município.

IV – Riscos Operacionais

a) execução inadequada de obrigações da PARCEIRA;
b) indisponibilidade de equipe;
c) atrasos em entregas ou marcos;
d) problemas com ambientes ou infraestrutura.

V – Riscos de Mercado

a) baixa adesão de clientes externos;
b) variações no modelo de negócios;
c) mudanças no ambiente competitivo;
d) crises econômicas.

VI – Riscos Regulatórios e Institucionais

a) mudanças legislativas;
b) exigências de novos padrões de conformidade;
c) restrições de órgãos de controle;
d) impactos urbanos e regulatórios em cidades inteligentes.

VII – Riscos Financeiros

a) inadimplência de clientes;
b) desbalanceamento de aportes;
c) custos extraordinários não previstos.

13.4 – Alocação de Riscos entre as PARCEIRAS

14.4.1. Os riscos serão alocados conforme:

I – a natureza da contribuição técnica de cada PARCEIRA;
II – responsabilidades específicas previstas no PNO;
III – a capacidade de mitigação de cada PARCEIRA;
IV – a Matriz de Riscos;
V – o princípio da proporcionalidade contributiva.

14.4.2. Em regra:

a) riscos ligados à arquitetura municipal, dados municipais, infraestrutura pública são alocados à PRODAM;
b) riscos ligados a código, módulos, entregas, APIs, desenvolvimentos e integrações da PARCEIRA são alocados à PARCEIRA;
c) riscos compartilhados serão tratados na governança da ON.

14.4.3. A PARCEIRA responderá integralmente por riscos decorrentes de:

I – falhas próprias;
II – descumprimento de obrigações deste Contrato;
III – violação de segurança ou integridade atribuível a sua atuação;
IV – erros de implementação, desenvolvimento ou integração;
V – má execução técnica ou negligência.

14.5 – Governança da Gestão de Riscos

14.5.1. A gestão da Matriz de Riscos será exercida pelo:

I – Gestor da Parceria (PRODAM);
II – Fiscal(is) da Parceria;
III – Comitê de Governança da ON;

IV – especialistas de segurança da PRODAM, quando aplicável.

14.5.2. Caberá à governança:

a) monitorar riscos registrados;
b) atualizar a matriz periodicamente;
c) aprovar medidas de mitigação;
d) reavaliar impactos e probabilidades;
e) deliberar sobre riscos emergentes.

14.6 – Atualização da Matriz de Riscos

14.6.1. A Matriz de Riscos poderá ser atualizada:

I – trimestralmente;
II – antes da liberação de módulos críticos;
III – após incidentes relevantes;
IV – quando houver evolução tecnológica da solução;
V – diante de novos ambientes regulatórios ou de mercado;
VI – sempre que o Comitê de Governança entender necessário.

14.6.2. A atualização não configura aditivo contratual, salvo quando implicar:

a) mudança de objeto;
b) transferência indevida de responsabilidades;
c) alteração de alocação essencial de riscos.

14.7 – Eventos de Risco e Resposta a Incidentes

14.7.1. Sempre que ocorrer evento de risco, a PARCEIRA responsável deverá:

I – comunicar imediatamente a PRODAM;
II – adotar medidas emergenciais de contenção;
III – registrar tecnicamente o ocorrido;
IV – propor ações corretivas e preventivas;
V – cooperar com auditorias e análises forenses;
VI – apresentar relatório de incidente em até 48 horas.

14.7.2. A governança da ON poderá:

a) determinar mitigação adicional;
b) suspender atividades;
c) exigir substituição de equipe;
d) solicitar auditorias externas;
e) atualizar a Matriz de Riscos.

14.8 – Responsabilidade por Danos Decorrentes de Riscos

14.8.1. Cada PARCEIRA responderá:

I – pelos danos decorrentes de riscos sob sua responsabilidade;
II – pela reparação integral dos prejuízos causados à ON, à PRODAM ou a terceiros;
III – pelas penalidades contratuais e legais aplicáveis.

14.8.2. Danos decorrentes de riscos compartilhados serão tratados conforme regras definidas no PNO e na governança da ON.

14.9 – Reversão de Riscos e Sustentação Operacional

14.9.1. Em caso de incapacidade temporária ou permanente da PARCEIRA de mitigar ou suportar determinado risco, a PRODAM poderá:

I – assumir temporariamente as atividades críticas;
II – contratar terceiros para contenção e continuidade;
III – acionar mecanismos de resiliência previstos no PNO.

13.9.2. Os custos decorrentes da falha da PARCEIRA serão de sua responsabilidade, nos termos desta cláusula.

CLÁUSULA 15 – GARANTIAS

15.1 – Garantia da Execução e Cumprimento das Obrigações

15.1.1. Cada PARCEIRA garante, pelo presente instrumento, o cumprimento integral e diligente de todas as obrigações assumidas neste Contrato, no PNO, no PNPO, na Matriz de Riscos e nos documentos integrantes da Oportunidade de Negócio SMARTSAMPA.

15.1.2. Constituem garantias de execução por parte de cada PARCEIRA:

I – a alocação de equipe técnica qualificada;
II – a manutenção de capacidade operacional, tecnológica e organizacional compatível com as obrigações assumidas;
III – o atendimento aos requisitos de governança, compliance, integridade e segurança da informação;
IV – o uso adequado dos ativos e recursos necessários à ON;
V – a manutenção das condições de habilitação técnica e jurídica durante toda a vigência.

15.2 – Garantia de Integridade e Conformidade

15.2.1. A PARCEIRA garante que:

I – manterá seu Programa de Integridade ativo, atualizado e funcional;
II – cumprirá integralmente a LGPD, a Lei nº 12.846/2013, a Lei nº 13.303/2016 e políticas da PRODAM;
III – não praticará atos de corrupção, fraude, conluio, favorecimento, tráfico de influência ou qualquer prática proibida;
IV – manterá rigoroso controle interno sobre riscos operacionais, regulatórios, técnicos e de integridade;
V – não se encontra impedida de contratar com a Administração Pública.

15.2.2. A violação desse item constitui infração gravíssima sujeita às penalidades contratuais e legais.

15.3 – Garantia de Propriedade Intelectual e Não Violação

15.3.1. A PARCEIRA garante que os ativos tecnológicos, módulos, códigos e integrações por ela disponibilizados:

I – não violam direitos autorais, patentes, segredos de negócio ou quaisquer direitos de terceiros;
II – não utilizam componentes ilícitos, não licenciados ou com restrições incompatíveis com este Contrato;
III – não infringem termos de licenciamento de softwares, frameworks ou bibliotecas externas;
IV – são entregues livres de ônus, reivindicações ou quaisquer gravames.

15.3.2. A PARCEIRA será exclusivamente responsável por danos e prejuízos decorrentes de violação de propriedade intelectual de terceiros.

15.4 – Garantia de Continuidade Operacional

15.4.1. As PARCEIRAS garantem que adotarão medidas para assegurar a continuidade operacional da solução SMARTSAMPA, observando:

I – redundância mínima operacional;
II – controles de segurança apropriados;
III – manutenção de ambientes críticos;
IV – resposta a incidentes;
V – atualização tecnológica periódica;
VI – suporte técnico emergencial em caso de falhas ou indisponibilidades.

15.4.2. Caso qualquer PARCEIRA enfrente evento que comprometa a continuidade, deverá comunicar imediatamente à governança da ON e adotar ações corretivas.

15.5 – Garantia de Confidencialidade e Segurança da Informação

15.5.1. As PARCEIRAS garantem:

I – a guarda, proteção e integridade das Informações Sigilosas;
II – a adoção de medidas técnicas e administrativas de proteção;
III – o cumprimento das políticas internas da PRODAM de segurança da informação;
IV – a pronta comunicação de incidentes;
V – o sigilo absoluto sobre informações estratégicas, documentações e dados municipais.

15.6 – Garantia de Manutenção de Condições Habilitatórias

15.6.1. Durante toda a vigência do Contrato, as PARCEIRAS garantem que manterão:

I – regularidade fiscal e trabalhista;
II – capacidade técnica compatível;
III – qualificação jurídica necessária;
IV – ausência de sanções impeditivas;
V – habilitação societária e operacional adequada.

15.6.2. Qualquer alteração relevante deverá ser comunicada imediatamente à governança da ON.

15.7 – Garantia de Veracidade das Informações Prestadas

15.7.1. As PARCEIRAS garantem que todas as declarações, documentos, dados, informações e manifestações prestadas no processo da ON são:

I – verdadeiras;
II – completas;
III – auditáveis;
IV – coerentes com suas operações reais.

15.7.2. A prestação de informações falsas constitui causa de rescisão imediata.

15.8 – Garantia Operacional da PARCEIRA

15.8.1. A PARCEIRA garante que:

I – possui capacidade técnica para cumprir as obrigações atribuídas;
II – dispõe de infraestrutura compatível com o SMARTSAMPA;
III – manterá profissionais qualificados;
IV – atuará conforme padrões de qualidade definidos no PNO;
V – assumirá os riscos técnicos das entregas sob sua responsabilidade.

15.9 – Garantia da PRODAM como Líder Institucional da ON

15.9.1. A PRODAM garante que:

I – atuará como agente público coordenador da ON;
II – proverá acesso autorizado às bases e sistemas municipais quando necessário;
III – manterá sua capacidade institucional durante a vigência;
IV – executará suas funções de governança e fiscalização;
V – assegurará condições de continuidade no âmbito institucional.

CLÁUSULA 16 – RESPONSABILIDADE DAS PARTES

16.1 – Responsabilidade Geral

16.1.1. Cada PARCEIRA será exclusivamente responsável por seus atos, omissões, decisões, atividades técnicas, operacionais, administrativas, tecnológicas e regulatórias realizadas no âmbito deste Contrato.

16.1.2. A responsabilidade de cada PARCEIRA será apurada de acordo com:

I – suas obrigações contratuais;
II – sua contribuição técnica e operacional;
III – a alocação de riscos definida na Matriz de Riscos;
IV – o PNO e seus anexos;
V – a legislação aplicável.

16.2 – Ausência de Solidariedade

16.2.1. Este Contrato, por sua natureza associativa, não gera:

I – vínculo de solidariedade entre as PARCEIRAS;
II – assunção de dívidas ou obrigações da outra PARCEIRA;
III – responsabilidade conjunta por obrigações fiscais, trabalhistas ou empresariais;
IV – corresponsabilidade automática por falhas técnicas alheias.

16.2.2. Cada PARCEIRA responderá pelos danos decorrentes de suas próprias ações, sem prejuízo da responsabilidade compartilhada prevista em Matriz de Riscos, quando aplicável.

16.3 – Responsabilidade da PARCEIRA

16.3.1. A PARCEIRA será integralmente responsável por:

I – entrega, qualidade, desempenho, estabilidade e segurança dos módulos, códigos, integrações, algoritmos, APIs e artefatos sob sua responsabilidade;
II – falhas técnicas, erros de desenvolvimento, vulnerabilidades, indisponibilidades ou mau funcionamento decorrentes de sua atuação;

III – violação de dados pessoais, dados sensíveis, dados municipais ou informações sigilosas por sua equipe, prepostos, fornecedores ou subcontratados;
IV – multas, sanções ou danos decorrentes do uso indevido de bases municipais, arquiteturas internas ou Informações Sigilosas;
V – prejuízos causados por descumprimento da LGPD, da Lei 12.846/2013, ou de normas de integridade e governança;
VI – violações de propriedade intelectual de terceiros decorrentes de seu código, bibliotecas, frameworks ou dependências;
VII – incidentes decorrentes de falhas de segurança da informação atribuíveis à sua atuação.

16.3.2. A PARCEIRA responderá ainda pela conduta:

a) de seus empregados;
b) de terceiros sob sua supervisão;
c) de fornecedores que atuarão no âmbito da ON;
d) de subcontratados, quando autorizados.

16.4 – Responsabilidade da PRODAM

16.4.1. A PRODAM será responsável por:

I – informações, bases, dados e ambientes internos que disponibilizar;
II – integridade institucional da governança e da condução da ON;
III – falhas em sistemas municipais de sua responsabilidade exclusiva;
IV – indisponibilidades de infraestrutura pública atribuíveis à PRODAM;
V – incidentes decorrentes de dados municipais cuja custódia seja de sua competência;
VI – rotinas internas de segurança, classificação e autorização de acesso.

16.4.2. A PRODAM não será responsável:

I – por falhas de código, arquitetura ou módulos desenvolvidos pela PARCEIRA;
II – por danos decorrentes de descumprimento contratual da PARCEIRA;
III – por decisões técnicas, comerciais ou operacionais exclusivamente atribuídas à PARCEIRA;
IV – por danos decorrentes de atos ilícitos praticados pela PARCEIRA ou seus representantes.

16.5 – Responsabilidade Conjunta (quando prevista pela Matriz de Riscos)

16.5.1. Quando a Matriz de Riscos determinar responsabilidade compartilhada, as PARCEIRAS responderão:

I – de forma proporcional à sua contribuição;
II – conforme critérios definidos no PNO;
III – mediante deliberação do Comitê de Governança.

16.5.2. Mesmo nos riscos compartilhados, não há solidariedade automática.

16.6 – Limitação de Responsabilidade

16.6.1. Não haverá limitação de responsabilidade quando o dano decorrer de:

I – dolo ou fraude;
II – má-fé;
III – violação de dados pessoais;
IV – violação de Informações Sigilosas;
V – atos de corrupção, conluio ou práticas antiéticas;
VI – violação de propriedade intelectual;
VII – atos que impliquem risco à segurança pública ou à infraestrutura crítica da cidade;
VIII – violação grave de obrigações de segurança da informação.

16.6.2. Nos demais casos, e se tecnicamente aplicável, limites poderão ser definidos no PNO.

16.7 – Danos Indiretos, Lucros Cessantes e Danos por Terceiros

16.7.1. As PARCEIRAS não responderão por danos indiretos (perdas de oportunidade, danos morais, lucros cessantes), salvo quando tais danos:

I – decorrerem de conduta dolosa;
II – envolverem dados pessoais ou sigilosos;
III – resultarem de incidente de segurança atribuível à conduta da parte;
IV – forem consequência direta e imediata de descumprimento contratual;
V – estiverem previstos na Matriz de Riscos.

16.7.2. A PARCEIRA responderá integralmente por danos:

a) causados a Clientes;
b) decorrentes de uso indevido da marca SMARTSAMPA;
c) resultantes de falhas técnicas de sua responsabilidade.

16.8 – Responsabilidade perante Órgãos de Controle

16.8.1. Cada PARCEIRA responderá individualmente perante:

I – Controladoria Geral do Município;
II – Tribunal de Contas do Município;
III – Ministério Público;
IV – demais órgãos competentes;

pela parte que lhe couber nos fatos sob análise.

16.9 – Responsabilidade pela Equipe, Subcontratados e Terceiros

16.9.1. Cada PARCEIRA é inteiramente responsável:

I – por sua equipe técnica;
II – por atos, erros, omissões, condutas e qualificações de seus fornecedores e terceiros;
III – por obrigações trabalhistas, previdenciárias, fiscais e securitárias;
IV – pelo cumprimento de normas de integridade por seus colaboradores.

16.10 – Cooperação para Mitigação de Danos

16.10.1. As PARCEIRAS deverão:

I – atuar de forma cooperativa para reduzir impactos de incidentes;
II – adotar medidas emergenciais para mitigar riscos;
III – compartilhar informações técnicas necessárias à contenção de danos;
IV – registrar evidências e comunicações no processo da ON.

CLÁUSULA 17 – PENALIDADES

17.1 – Natureza das Penalidades

17.1.1. As penalidades previstas nesta Cláusula destinam-se a assegurar:

I – o cumprimento das obrigações técnicas e de governança;
II – a integridade da solução SMARTSAMPA;
III – a mitigação de riscos relevantes;
IV – a proteção das Informações Sigilosas e dos dados municipais;
V – a continuidade operacional da ON;
VI – a observância dos princípios previstos no RPON-PRODAM.

17.1.2. A aplicação das penalidades não possui natureza remuneratória, não implica contraprestação e não descaracteriza a natureza associativa deste Contrato.

17.2 – Hipóteses de Infração

Constituem infrações, sem prejuízo de outras previstas no Contrato, na Matriz de Riscos e na legislação aplicável:

I – descumprimento de obrigações técnicas ou operacionais atribuídas à PARCEIRA;
II – atraso injustificado em entregas, marcos ou atividades críticas do PNO;
III – falhas de segurança da informação atribuíveis à PARCEIRA;
IV – violação de Informações Sigilosas ou dados municipais;
V – violação da LGPD, Lei 12.846/2013 ou políticas de integridade;
VI – uso não autorizado de ativos da ON;
VII – violação de propriedade intelectual;

VIII – condutas que comprometam a governança da ON;
IX – omissão, fraude, declaração falsa ou manipulação de dados;
X – prática de atos ilícitos, antiéticos ou incompatíveis com o Programa de Integridade da PRODAM;
XI – reincidência de falhas técnicas;
XII – não observância da Matriz de Riscos;
XIII – negativa injustificada de fornecer informações auditáveis.

17.3 – Modalidades de Penalidades

A depender da gravidade, impacto, reincidência e responsabilidade da infração, poderão ser aplicadas, isolada ou cumulativamente, as seguintes penalidades:

I – Advertência Formal

17.3.1. Aplicável a infrações de baixo impacto, sujeita à correção imediata.

II – Determinações Técnicas Obrigatórias

17.3.2. A governança da ON poderá determinar:

a) ajustes técnicos;
b) correções de código;
c) reforço de segurança;
d) substituição de equipe;
e) revisão de documentação;
f) entrega de relatórios adicionais;
g) implementação de medidas de mitigação.

III – Suspensão Temporária de Acessos

17.3.3. Em caso de risco relevante ou infração de gravidade média, poderá ser determinada a suspensão parcial ou total de acessos:

I – a ambientes de homologação;
II – a ambientes de produção;
III – a dados municipais;
IV – a APIs e integrações.

Suspensão não exime a PARCEIRA de responsabilidade.

IV – Bloqueio de Entregas e Marcos

17.3.4. Em caso de descumprimento de obrigações técnicas essenciais, a governança poderá bloquear a entrega de novos módulos até a regularização.

V – Substituição de Equipe Técnica

17.3.5. A PRODAM poderá exigir substituição imediata de membros da equipe que:

I – demonstrem conduta inadequada;
II – não possuam qualificação técnica necessária;
III – comprometam a segurança, integridade ou operação.

VI – Restrição à Participação em Etapas da ON

17.3.6. A PARCEIRA poderá ser impedida de participar de fases específicas da ON quando sua atuação representar risco.

VII – Impedimento de Exploração Econômica

17.3.7. Em casos graves, a PARCEIRA poderá ter bloqueada sua participação no rateio de receitas referentes ao período de ocorrência da infração, quando:

I – a infração gerar dano econômico à ON;
II – houver violação de integridade;
III – houver prejuízo comprovado à exploração comercial da solução.

VIII – Descontinuidade Técnica ou Operacional da PARCEIRA

17.3.8. A governança poderá determinar a substituição da PARCEIRA em atividades críticas, inclusive:

I – assumindo temporariamente a operação;
II – contratando terceiros;
III – redistribuindo obrigações conforme o PNO.

IX – Rescisão do Contrato

17.3.9. A rescisão poderá ocorrer nas hipóteses previstas na Cláusula de Rescisão, especialmente por:

I – incidente grave de segurança;
II – violação de dados pessoais;
III – ato de corrupção ou fraude;
IV – violação de Informações Sigilosas;
V – violação de propriedade intelectual;
VI – uso indevido da marca SMARTSAMPA;
VII – descumprimento material do contrato.

17.4 – Procedimento para Aplicação das Penalidades

17.4.1. A aplicação de penalidades observará:

I – contraditório e ampla defesa;
II – análise técnica fundamentada;
III – registro formal no processo administrativo da ON;
IV – deliberação da governança, quando aplicável.

17.4.2. A PARCEIRA deverá apresentar justificativa técnica no prazo de 5 (cinco) dias úteis, prorrogável mediante justificativa.

17.4.3. A decisão será comunicada formalmente à PARCEIRA, com indicação:

a) da infração;
b) dos fatos relevantes;
c) da penalidade aplicada;
d) das medidas corretivas exigidas.

17.5 – Reincidência

16.5.1. A reincidência, independentemente do tipo de infração, autoriza a aplicação de penalidade mais grave.

17.6 – Cumulação de Penalidades

17.6.1. Penalidades podem ser aplicadas cumulativamente quando:

I – a infração tiver múltiplos impactos;
II – houver combinação de falhas técnicas e de integridade;
III – a matriz de risco indicar gravidade elevada.

17.7 – Ausência de Indenização Automática

17.7.1. A aplicação de penalidade não exclui a obrigação de indenizar a PRODAM ou terceiros pelos danos causados.

CLÁUSULA 18 – VIGÊNCIA E RESCISÃO

18.1 – Vigência

18.1.1. O presente Contrato terá vigência de 60 (sessenta) meses contados da data de sua assinatura, podendo ser prorrogado mediante:

I – manifestação justificada da governança da Oportunidade de Negócio SMARTSAMPA;
II – avaliação técnica e estratégica da PRODAM;
III – assinatura de termo aditivo.

18.1.2. A vigência poderá ser prorrogada sucessivamente enquanto:

a) houver continuidade operacional da solução;
b) a parceria gerar resultados e oportunidades;
c) não houver impedimentos legais, regulatórios ou institucionais;
d) o modelo de negócios permanecer ativo.

18.2 – Término Natural da Vigência

18.2.1. O Contrato poderá ser encerrado ao final de sua vigência mediante:

I – conclusão da Oportunidade de Negócio;
II – encerramento da exploração econômica do SMARTSAMPA;
III – decisão fundamentada da governança da ON.

18.2.2. O encerramento natural não exime as PARCEIRAS:

a) do dever de confidencialidade (vigência prolongada pela Cláusula 12);
b) da responsabilidade por danos;
c) das obrigações referentes à propriedade intelectual conjunta;
d) da entrega de documentação e ativos devidos.

18.3 – Hipóteses de Rescisão

O Contrato poderá ser rescindido:

I – Por Acordo entre as Partes

18.3.1. Mediante instrumento escrito, desde que:

a) preservada a continuidade da solução;
b) definida a transferência de ativos conjuntos;
c) regulado o encerramento das obrigações do PNO.

II – Por Iniciativa da PRODAM (rescisão unilateral)

18.3.2. A PRODAM poderá rescindir unilateralmente, mediante notificação, quando a PARCEIRA:

I – violar dados pessoais, dados sensíveis ou dados municipais;
II – comprometer a segurança da informação ou infraestrutura crítica;

III – violar Informações Sigilosas;
IV – praticar atos de corrupção, fraude, conluio, conflito de interesse ou práticas incompatíveis com integridade;
V – descumprir obrigações técnicas essenciais;
VI – reincidir em falhas classificadas como graves;
VII – violar direitos de propriedade intelectual;
VIII – interromper injustificadamente a execução de suas obrigações;
IX – tiver sua habilitação jurídica, técnica ou fiscal comprometida;
X – tornar-se inidônea ou impedida de contratar com a Administração Pública;
XI – causar dano material à ON, à PRODAM ou a Clientes.

III – Por Iniciativa da PARCEIRA (rescisão unilateral)

18.3.3. A PARCEIRA poderá rescindir unilateralmente caso:

I – a PRODAM descumpra obrigações essenciais sob sua responsabilidade;
II – haja alteração substancial no PNO sem justificativa técnica;
III – surjam impedimentos legais que inviabilizem sua participação.

18.3.4. A rescisão pela PARCEIRA não poderá ocorrer:

a) sem prévia comunicação;
b) sem participação da governança da ON;
c) sem assegurar continuidade mínima da solução.

IV – Rescisão por Caso Fortuito ou Força Maior

18.3.5. Poderá ocorrer quando o evento:

I – for imprevisível ou inevitável;
II – comprometer integralmente a execução da ON;
III – impossibilitar a continuidade da parceria.

18.3.6. A parte afetada deverá:

a) comunicar imediatamente;
b) adotar medidas mitigadoras;
c) comprovar documentalmente o evento.

V – Rescisão por Órgãos de Controle ou Determinação Legal

18.3.7. O Contrato poderá ser rescindido se:

I – houver determinação judicial;
II – houver decisão de órgão de controle externo ou interno;

III – normas legais supervenientes tornarem a ON inviável.

18.4 – Procedimento de Rescisão

18.4.1. Salvo nas hipóteses graves previstas nesta cláusula, a parte interessada notificará a outra PARCEIRA com antecedência mínima de 30 (trinta) dias, apresentando:

I – fundamentos;
II – fatos relevantes;
III – efeitos esperados;
IV – propostas de transição.

18.4.2. A governança da ON poderá recomendar:

a) ajustes ou medidas mitigadoras;
b) continuidade condicionada a correções;
c) rescisão imediata quando houver risco relevante.

18.5 – Efeitos da Rescisão

Com a rescisão, independentemente do motivo:

I – Entrega e Transferência de Ativos Conjuntos

18.5.1. A PARCEIRA deverá entregar à PRODAM:

I – todo ativo conjunto (PI compartilhada);
II – documentações, códigos, diagramas, fluxos e manuais;
III – versões estáveis da solução;
IV – materiais técnicos produzidos;
V – relatórios de pendências e riscos.

II – Continuidade Operacional

18.5.2. A PARCEIRA deverá garantir continuidade por até 90 dias, abrangendo:

a) suporte técnico emergencial;
b) transferência de conhecimento (knowledge transfer);
c) assistência na transição para terceiros ou para a PRODAM;
d) esclarecimento de componentes críticos.

III – Cessação de Direitos

18.5.3. Com a rescisão:

I – cessam licenças concedidas, salvo para operação da solução conjunta;
II – cessam acessos a dados, sistemas e ambientes;
III – ficam suspensas participações em receitas futuras;

sem prejuízo da continuidade de uso dos ativos conjuntos pela PRODAM.

IV – Responsabilidade por Danos

18.5.4. A rescisão não extingue:

a) obrigações de indenizar;
b) obrigações de confidencialidade;
c) obrigações relativas à integridade;
d) obrigações relativas à propriedade intelectual;
e) responsabilidades atribuídas pela Matriz de Riscos.

18.6 – Irregularidades Grave e Rescisão Imediata

18.6.1. A rescisão poderá ser imediata, sem prazo de transição, quando houver:

I – violação grave de dados pessoais ou sigilosos;
II – risco à segurança pública ou aos sistemas municipais;
III – fraude, corrupção, conluio ou ilícito relevante;
IV – violação intencional de propriedade intelectual;
V – dano material grave à ON;
VI – ato doloso com prejuízo direto à PRODAM.

18.6.2. Mesmo na rescisão imediata, permanecem vigentes todas as obrigações de confidencialidade, integridade e transferência de ativos conjuntos.

CLÁUSULA 19 – SOLUÇÃO DE CONTROVÉRSIAS

19.1 – Princípio Geral

19.1.1. As PARCEIRAS envidarão seus melhores esforços para resolver, de forma consensual e cooperativa, quaisquer divergências, dúvidas, conflitos ou controvérsias relacionadas à interpretação ou execução deste Contrato, do PNO, do PNPO, da Matriz de Riscos ou de qualquer documento da Oportunidade de Negócio SMARTSAMPA.

19.2 – Etapa Obrigatória: Solução pela Governança da ON

19.2.1. Qualquer controvérsia deverá, obrigatoriamente, ser inicialmente submetida ao:

I – Gestor da Parceria (PRODAM);
II – Fiscal(is) da Parceria;

III – Comitê de Governança da ON.

19.2.2. A governança analisará:

a) fatos e documentos;
b) aspectos técnicos;
c) alocação de riscos;
d) responsabilidades atribuídas;
e) impacto da controvérsia na solução.

19.2.3. A governança deverá emitir deliberação fundamentada no prazo de 30 (trinta) dias, prorrogável mediante justificativa.

19.3 – Etapa Técnica: Câmaras Técnicas ou Consultoria Especializada

19.3.1. Caso a controvérsia envolva matéria técnica complexa, poderá a governança da ON determinar:

I – análise por Câmara Técnica da PRODAM;
II – parecer de especialistas internos;
III – realização de testes, benchmarks ou perícias técnicas;
IV – contratação de consultoria independente, se necessário.

19.3.2. O custo de eventual perícia externa será:

I – rateado entre as PARCEIRAS quando a responsabilidade for indeterminada;
II – suportado exclusivamente pela PARCEIRA responsável, quando comprovado o descumprimento.

19.4 – Etapa Consensual: Mediação

19.4.1. Persistindo a controvérsia após a etapa de governança, as PARCEIRAS concordam em submeter o conflito à mediação, preferencialmente na Câmara de Mediação da Administração Pública Municipal, quando existente.

19.4.2. A mediação não terá caráter obrigatório, mas será priorizada para evitar judicialização.

19.5 – Etapa Normativa: Órgãos de Controle

19.5.1. Em caso de controvérsia relativa a:

I – integridade;
II – risco sistêmico;
III – dados municipais;
IV – segurança da informação;

V – ou impactos relevantes na Administração Pública;

poderão ser consultados, conforme o caso:

a) Controladoria Geral do Município;
b) Procuradoria Geral do Município;
c) Auditoria Interna da PRODAM.

19.6 – Etapa Final: Poder Judiciário

19.6.1. Não sendo possível a solução consensual ou técnica, a controvérsia poderá ser submetida ao Poder Judiciário, conforme foro definido na cláusula final.

19.6.2. A judicialização não afasta:

I – obrigações de continuidade;
II – dever de entrega de ativos conjuntos;
III – obrigações de segurança;
IV – incidência do PNO e da Matriz de Riscos.

19.7 – Continuidade da Execução Durante a Controvérsia

19.7.1. Durante qualquer controvérsia, as PARCEIRAS deverão:

I – assegurar a continuidade da solução SMARTSAMPA;
II – manter a execução das obrigações contratuais;
III – adotar medidas emergenciais determinadas pela governança da ON;
IV – evitar soluções que possam comprometer o serviço ou os dados municipais.

19.8 – Caráter Não Remuneratório

19.8.1. A submissão de controvérsias às etapas descritas nesta cláusula:

I – não configura prestação de serviços;
II – não implica contraprestação financeira;
III – respeita a natureza associativa do contrato.

19.9 – Registro e Transparência

19.9.1. Todas as comunicações, deliberações e decisões relativas à controvérsia deverão:

I – ser registradas no processo administrativo da ON;
II – manter trilha de auditoria;
III – observar sigilo, quando cabível.

CLÁUSULA 20 – DISPOSIÇÕES GERAIS

20.1 – Natureza Associativa

20.1.1. O presente Contrato tem natureza estritamente associativa, não estabelecendo vínculo de fornecimento, prestação de serviços, terceirização, sociedade, mandato, consórcio, joint venture, representação comercial, franquia ou qualquer forma de relação remuneratória entre as PARCEIRAS.

20.1.2. Cada PARCEIRA atua de forma autônoma e independente, respondendo exclusivamente por seus próprios atos.

20.2 – Ausência de Vínculo Trabalhista

20.2.1. A execução deste Contrato não gera vínculo trabalhista entre:

I – colaboradores, empregados, prepostos ou representantes da PARCEIRA e a PRODAM;
II – colaboradores da PRODAM e a PARCEIRA.

20.2.2. Cada PARCEIRA será exclusivamente responsável por eventuais encargos trabalhistas, previdenciários, fiscais, securitários ou de qualquer natureza referentes às pessoas sob sua responsabilidade.

20.3 – Documentos Integrantes

20.3.1. Fazem parte indissociável deste Contrato:

I – PNPO – Plano de Negócio da Parceria;
II – PNO – Plano da Oportunidade de Negócio;
III – Matriz de Riscos;
IV – Plano de Governança;
V – documentos e deliberações formais da ON;
VI – anexos específicos definidos no instrumento.

20.3.2. Em caso de conflito entre documentos:

I – prevalecerá o texto deste Contrato;
II – na sequência, o PNO;
III – depois, a Matriz de Riscos;
IV – e, por fim, o PNPO.

20.4 – Subcontratação

20.4.1. A PARCEIRA somente poderá subcontratar atividades:

I – autorizadas previamente pela PRODAM;
II – de natureza acessória e complementar;
III – que não comprometam a segurança da informação ou dados municipais;
IV – desde que o subcontratado assine termos de confidencialidade equivalentes.

20.4.2. A subcontratação não transfere responsabilidade, permanecendo a PARCEIRA inteiramente responsável:

a) pelos atos do subcontratado;
b) pela qualidade, segurança e continuidade das atividades;
c) pelas obrigações trabalhistas, fiscais e previdenciárias do subcontratado.

20.5 – Cessão, Transferência e Alteração Societária

20.5.1. É vedada a cessão ou transferência deste Contrato, total ou parcial, sem autorização prévia e escrita da PRODAM.

20.5.2. A PARCEIRA deverá comunicar à PRODAM quaisquer alterações societárias relevantes, incluindo:

I – mudança de controle;
II – reorganização societária;
III – fusão, incorporação ou cisão;
IV – entrada de sócios estratégicos.

20.5.3. A PRODAM poderá exigir comprovação de que a PARCEIRA mantém:

a) habilitação técnica;
b) integridade institucional;
c) capacidade operacional;
d) ausência de impedimentos legais.

20.6 – Publicidade e Transparência

20.6.1. As PARCEIRAS deverão observar:

I – o dever constitucional de publicidade;
II – a transparência dos atos administrativos;
III – normas de acesso à informação;
IV – limites legais de sigilo técnico, comercial e de segurança.

20.6.2. O uso de logotipos, marcas, nomes e elementos visuais da PRODAM ou do SMARTSAMPA depende de autorização prévia e escrita.

20.7 – Comunicação e Notificações

20.7.1. Todas as comunicações, notificações, avisos e solicitações deverão ser realizadas:

I – por meio do processo administrativo eletrônico do Município (SEI);
II – ou por e-mail institucional cadastrado no processo da ON;
III – ou por outro meio institucional admitido pela PRODAM.

20.7.2. Notificações formais considerar-se-ão entregues:

a) no momento do registro no SEI;
b) ou após confirmação automática de recebimento em e-mail institucional.

20.8 – Inexistência de Exclusividade

20.8.1. Salvo se expressamente previsto, nenhuma das PARCEIRAS detém exclusividade:

I – para comercialização;
II – para exploração comercial externa;
III – para participação futura em módulos ou evoluções.

20.8.2. A PRODAM poderá celebrar parcerias complementares, desde que não haja conflito com este Contrato.

20.9 – Interpretação e Prevalência

20.9.1. Este Contrato deve ser interpretado conforme:

I – seu caráter associativo;
II – o RPON-PRODAM;
III – as políticas internas da PRODAM;
IV – os princípios da boa-fé, cooperação e integridade.

20.9.2. Em caso de ambiguidade, prevalece a interpretação que:

a) preserve a segurança do SMARTSAMPA;
b) favoreça a governança pública;
c) proteja dados municipais e ativos estratégicos;
d) assegure continuidade da solução.

20.10 – Alterações Contratuais

20.10.1. O Contrato poderá ser alterado mediante termo aditivo, desde que:

I – aprovado pela governança da ON;
II – tecnicamente justificado;

III – não haja descaracterização do modelo associativo;
IV – seja registrado no processo administrativo correspondente.

20.11 – Tolerância e Renúncia

20.11.1. O não exercício, tolerância ou atraso no exercício de qualquer direito não implica renúncia, podendo ser exercido a qualquer tempo durante a vigência do Contrato.

20.12 – Validade das Disposições

20.12.1. A nulidade de qualquer disposição deste Contrato não afetará as demais cláusulas, que permanecerão válidas e eficazes.

20.13 – Prevalência em Caso de Conflitos Internos

20.13.1. Em caso de conflito entre deliberações internas da PARCEIRA e disposições deste Contrato, prevalecerá o presente instrumento.

CLÁUSULA 21 – FORO

21.1 – Foro Competente

Para dirimir quaisquer controvérsias decorrentes da interpretação ou execução deste Contrato que não possam ser solucionadas pelas etapas de governança, solução consensual ou mediação previstas na Cláusula 18, fica eleito o Foro Central da Comarca da Capital do Estado de São Paulo, com renúncia a qualquer outro, por mais privilegiado que seja.

21.2 – Prorrogação da Competência

21.2.1. As PARCEIRAS reconhecem que a competência do foro ora eleito subsiste:

I – durante toda a vigência;
II – após o término do Contrato;
III – durante o período de obrigações remanescentes.

ANEXO A – TRATAMENTO DE DADOS PESSOAIS

1. Finalidade deste Anexo:

1.1. O presente Anexo detalha as obrigações operacionais, procedimentos, controles e instrumentos necessários para o adequado tratamento de Dados Pessoais e Dados Pessoais Sensíveis no âmbito da Oportunidade de Negócio SMARTSAMPA, em complemento direto à Cláusula 8 – Proteção de Dados e Segurança da Informação deste Contrato.

1.2. Este Anexo deve ser interpretado como extensão técnica da Cláusula 8, não criando regimes paralelos, mas especificando como tais obrigações serão executadas, documentadas e auditadas.

2. Papéis e Responsabilidades:

2.1. As PARCEIRAS reconhecem que os papéis de Controlador, Operador e Suboperador serão definidos caso a caso, conforme já previsto na Cláusula 8, especialmente em seu item 8.3, respeitando:

I – a finalidade do tratamento;
II – o ente responsável pela política pública ou serviço;
III – o instrumento jurídico firmado com o Cliente;
IV – os fluxos descritos no PNO.

2.2. Para fins operacionais, fica estabelecido que:

a) quando o tratamento decorrer de política pública municipal, o órgão público é, em regra, o Controlador;
b) a PRODAM atuará preferencialmente como Operadora;
c) a PARCEIRA atuará como Operadora ou Suboperadora, conforme o fluxo documental aprovado pela governança.

2.3. A definição final dos papéis será sempre registrada:

I – no PNO;
II – no contrato específico com Clientes (quando houver);
III – no processo administrativo da ON.

2.4. A PARCERIA deverá realizar semestralmente para cada projeto e cada Controlador

um Relatório de Impacto à Proteção de Dados (Data Protection Impact Assessment). Sendo uma documentação emitida pela PRODAM, a qual contém a descrição dos processos de tratamento de dados pessoais.
2.5. A PARCERIA deverá elaborar um Relatório de Impacto à Proteção de Dados (Data Protection Impact Assessment – RIPD) para cada projeto que envolva tratamento de dados pessoais, antes do início de sua execução. O documento será emitido pela PRODAM e deverá conter a descrição detalhada das operações de tratamento, finalidades, riscos identificados e medidas de mitigação adotadas.

3. Categorias de Dados e Finalidades:

3.1. As categorias de dados tratadas no âmbito da SMARTSAMPA serão aquelas estritamente necessárias para:

I – execução de políticas públicas relacionadas ao território, mobilidade, eventos urbanos, atendimento digital e demais serviços integrados;
II – operação do ecossistema digital SMARTSAMPA;
III – funcionalidades previstas no PNO ou instrumento correlato.

3.2. Cada fluxo relevante de dados deverá conter:

a) descrição da categoria de dados pessoais tratada;
b) finalidade específica;
c) base legal aplicável (item 8.4 da Cláusula 8);
d) indicação do operador responsável;
e) prazo de retenção;
f) critérios de eliminação ou anonimização.

3.3. O registro desses fluxos ocorrerá nos mapas de tratamento da ON e ficará disponível para consulta pela governança.

4. Bases Legais:

4.1. As bases legais previstas no item 8.4 da Cláusula 8 serão aplicadas conforme cada operação, devendo constar nos documentos:

I – PNO (versão vigente);
II – Plano de Governança;
III – instrumentos firmados com Clientes.

4.2. A mudança de base legal motivada por alteração de finalidade deverá ser previamente submetida à governança da ON.

5. Direitos dos Titulares (Complemento ao item 8.5)

5.1. Em cumprimento ao item 8.5 da Cláusula 8, cada PARCEIRA deverá manter mecanismos para atender, de forma rastreável, solicitações de titulares relativas a confirmação de tratamento, acesso, correção, anonimização, revogação de consentimento (quando aplicável), informação sobre compartilhamento, portabilidade (quando cabível).

5.2. O ponto de contato principal com o titular será o órgão público Controlador.
PRODAM e PARCEIRA prestarão suporte operacional mediante procedimentos definidos no PNO.

6. Compartilhamento de Dados:

6.1. Como complemento ao item 8.6, todo compartilhamento de dados pessoais com terceiros deverá:

I – ter base legal válida;
II – ser documentado no processo administrativo;
III – ser amparado por cláusulas contratuais equivalentes às deste Anexo e da Cláusula 8;
IV – estar previsto no PNO ou instrumento com o Cliente.

6.2. Operações que envolvam subcontratados exigem:

a) assinatura de Termo de Confidencialidade;
b) aceite das políticas de segurança da PRODAM;
c) aceite deste Anexo e da Cláusula 8.

7. Segurança da Informação:

7.1. Os controles previstos no item 8.7 serão detalhados operacionalmente:

I – no Plano de Governança da ON;
II – nos controles de acesso à solução SMARTSAMPA;
III – nos procedimentos de criptografia, autenticação, segregação e rastreabilidade;
IV – nos requisitos de proteção de dados territoriais e urbanos sensíveis.

7.2. A PARCEIRA compromete-se a implementar controles compatíveis com:

a) normas internas de segurança da PRODAM;
b) políticas de classificação de informação;

c) requisitos específicos do módulo da solução.

8. Incidentes de Segurança:

8.1. Incidentes descritos no item 8.8 deverão ser comunicados por escrito à outra PARCEIRA:

I – imediatamente, em até 24 horas após a ciência;
II – com informações suficientes para avaliação preliminar;
III – com atualização contínua até o encerramento do incidente.

8.2. A governança da ON será responsável por:

a) qualificar o impacto;
b) indicar medidas de mitigação;
c) decidir sobre comunicações obrigatórias à ANPD e titulares;
d) registrar todo o fluxo no processo administrativo.

9. Retenção e Eliminação de Dados:

9.1. Os prazos de retenção definidos no item 8.9 serão detalhados conforme:

I – contrato com Cliente;
II – legislação aplicável à política pública correlata;
III – requisitos do módulo da solução.

9.2. A eliminação ou anonimização deve:

a) ocorrer de forma segura;
b) ser documentada;
c) ser aprovada pela governança.

10. Transferência Internacional de Dados:

10.1. Qualquer operação tratada no item 8.10 exigirá:

I – avaliação de risco;
II – cláusulas contratuais específicas;
III – garantia de nível adequado de proteção;
IV – registro formal no processo administrativo da ON.

11. Encarregado (DPO) e Comunicação:

11.1. PRODAM e PARCEIRA deverão manter seus Encarregados atualizados no processo administrativo da ON.

11.2. As comunicações relacionadas a direitos de titulares, incidentes e avaliações de risco ocorrerão:

I – preferencialmente pelo SEI;
II – por e-mail institucional, quando necessário;
III – com rastreabilidade garantida.

12. Atualizações:
12.1. As atualizações previstas no item 8.12 serão incorporadas mediante:

I – deliberação da governança;
II – termo aditivo, quando necessário;
III – registro no processo da ON;
IV – comunicação às áreas técnicas envolvidas.

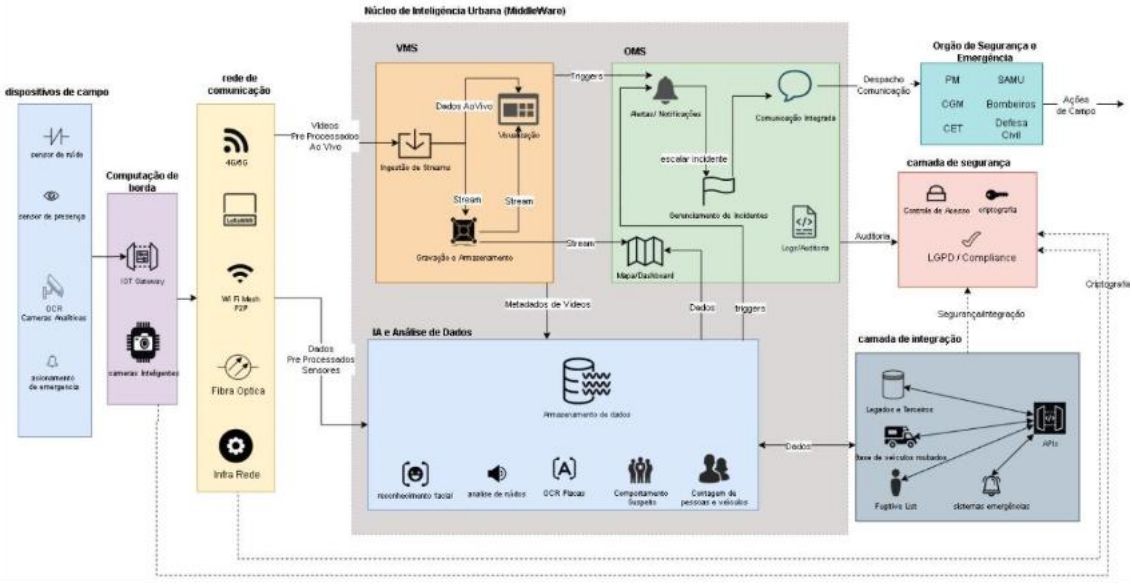
Anexo B -Descrição macro de módulos e funcionalidades

O presente documento busca detalhar as funcionalidades de uma solução de monitoramento e supervisão para a segurança pública urbana municipal, fortemente apoiada no uso de Inteligência Artificial na captura de dados e imagens ambientais via Visão Computacional, no reconhecimento facial e biométrico, no reconhecimento de comportamentos sociais, placas e características de veículo, sons, entre outros dados e metadados que possam alertar a segurança pública de eventos ou pessoas que possam ser interesse da ação tática.

Com o objetivo de:

I. Modernizar a gestão da segurança pública urbana,
II. Integrar dados e sistemas legados para análise operacional em tempo real.
III. Permitir respostas rápidas a incidentes através de uma central inteligente.
IV. Expandir futuramente para áreas como mobilidade urbana, meio ambiente e trânsito.
V. Estabelecer uma arquitetura replicável para qualquer município.

A plataforma chamada Smart Sampa PRODAM caracteriza-se pela modularidade e pelo atendimento às funcionalidades conforme apresentadas a seguir.



1. DISPOSITIVOS DE CAMPO:

Câmeras, sensores, dispositivos IoT integrados que fazem a captura de dados, imagens, vídeos, sons e metadados que possibilitam a classificação de interesse para a segurança pública. Parte desses dispositivos têm a capacidade de processamento na borda (Edge Computing) possibilitando o processamento em tempo real e a consequente aceleração dos disparos de ações pertinentes.

1. Captura por meio de câmeras, sensores e IoT.
2. Processamento e "cropping" de objetos de interesse.
3. Classificação inicial de interesse.
4. Transmissão e registro do objeto de interesse classificado.

Objetos de interesse incluem:

a. Monitoramento unificado em Tempo Real.
b. Reconhecimento facial e de padrões tal como placa de automóvel.
c. Reconhecimento de ocorrências e eventos no espaço público tais como dispersão em massa, enxameamento, abalroamento, queda de pessoas, luta corporal, entre outros.
d. Visão do espaço coberto pela câmera para efeito de pesquisa e exploração.
e. Detecção imediata de incidentes.

2. REDE DE COMUNICAÇÃO:

Utiliza diversas tecnologias como Fibra Óptica, Redes Móveis (4G/5G), LPWAN (LoRaWAN, NB-IoT) e Wi-Fi Mesh.

Garantir a conectividade entre os dispositivos e o tráfego de dados com os servidores de aplicação e dados. Atender às especificações técnicas, de disponibilidade e de banda necessárias e indicadas após os estudos e detalhamento de cada um dos pontos escolhidos.

3. MÓDULO VMS

1. Sistema de Gerenciamento de Vídeo (VMS): Responsável pela ingestão, gravação, armazenamento e reprodução (playback) dos fluxos de vídeo. Ele atua como fonte primária de dados de vídeo para o Centro de Controle e Sistema de

Despachos. Monitora e supervisiona o funcionamento dos dispositivos de campo gerando alertas caso reconheça falhas, indisponibilidades, vandalismo ou queda de conexão, entre outras anomalias possíveis. Gerencia o mapa e a localização de cada um dos dispositivos, assim como informações do entorno.

2. Gera e gerencia alertas automáticos de eventos suspeitos: Notificações automáticas baseadas em IA para eventos críticos, como detecção de procurados, desaparecidos, veículos roubados ou comportamentos suspeitos.
3. Indexa e gerencia os objetos gravados de modo a possibilitar a recuperação dentro das regras de armazenamentos definidas.
4. Visão Unificada da Cidade: Fornece uma visualização ao vivo e consolidada de todos os dispositivos (câmeras, sensores) em mapas interativos da cidade.

4. INTELIGÊNCIA ARTIFICIAL E ANALÍTICO DE DADOS

Módulos de Análise de Vídeo e Dados (IA/Data Analytics), com funcionalidades como reconhecimento facial e detecção de comportamento suspeito. Repositório de regras de análise e alarme criadas durante a operação. Módulo de Machine Learning para construção de novos padrões de reconhecimento, ação operacional ou controle.

1. Classificação do evento.
2. Determinação de criticidade
3. “Crop” de objetos de interesse
4. Clusterização de imagens e cenas com objetos de interesse coincidentes
5. Aprendizado de novos fenômenos ou padrões

5. SISTEMA DE GERENCIAMENTO DE EVENTOS E DESPACHO (OMS)

Centro de Controle Urbano – OMS (Operations Management System). Módulo responsável pelo envio ou despacho das ocorrências para os agentes operacionais, a saber, GCM, SAMU, Gestão de Trânsito, Assistência Social ou outros agentes escolhidos e indicados pelo poder municipal para responderem as demandas reconhecidas.

1. Plataforma central de orquestração das operações.
2. Dashboard Intuitivo.
3. Gestão das ocorrências e SLAs de cada uma delas.

4. Base de integração com os sistemas legados municipais.
5. Sistema de Alertas e Notificações.
6. Gestão dos VideoWalls e mapas em tempo real das ocorrências.
7. Gestão de Incidentes para classificação, despacho de equipes e acompanhamento de status.
8. Registro (LOG) de todas as operações despachadas e gestão dos históricos.
9. Geração de relatórios, painéis, dashboards ou consultas Ad-Hoc.
10. Plataforma intuitiva para a rápida tomada de decisão e o despacho de equipes para o local exato do incidente, incluindo GCM, Polícia Militar (PM), SAMU e órgãos de trânsito.
11. Comunicação Integrada: Permite comunicação direta e em tempo real com as equipes em campo (via rádio, aplicativos ou mensagens).
12. Geração de dados operacionais e estatísticos detalhados para otimizar o planejamento, alocação de recursos e a gestão contínua da segurança urbana.
13. Tomada de Decisão Baseada em Dados: Fornece informações precisas e insights preditivos para apoiar políticas públicas e estratégias urbanas.

6. CAMADA DE SEGURANÇA

1. Regras de manutenção e garantia da integração com Sistemas Legados e Terceiros.
2. Gestão dos perfis e dos históricos de acesso.
3. Adoção de regras e práticas sistêmicas para a garantia do compliance, validade, utilidade, consistência e sigilo das informações conforme determinado no regimento vigente.
4. Garante a conformidade com a LGPD e a privacidade de dados, incluindo Controle de Acesso e Criptografia.
5. Utiliza APIs e Protocolos Abertos para integração com bancos de dados de foragidos, veículos roubados e sistemas de trânsito.
7. CAMADA DE INTEGRAÇÃO E DISPONILIZAÇÃO DE DADOS

Conexão através de APIs e protocolos abertos com bancos de dados de foragidos, veículos roubados, sistemas de trânsito e centrais de emergência de órgãos de segurança, assim,

também com sistemas legados ou demandas por consumo de dados para efeito de planejamento, construção de estratégias, relatos e reports executivos e apoio operacional.

Risco	Definição	Alocação (público, privado ou compartilhado)	Impacto (alto, médio, baixo)	Probabilidade (frequente, provável, ocasional, remota ou improvável)	Mitigação (medidas, procedimentos ou mecanismos para minimizar)
Discrepância com preço de mercado	**Discrepância com preço de mercado** ocorre quando o **preço praticado** para um produto, serviço ou ativo financeiro é **diferente do valor geralmente aceito ou predominante no mercado**.	compartilhado	alto	ocasional	Monitoramento constante do mercado, ajuste de preços flexíveis.
Tecnologias emergentes	Tecnologias emergentes são inovações tecnológicas em estágio inicial de adoção, mas com alto potencial de transformação radical em setores, modelos de negócio e comportamentos. Elas representam novidades que podem mudar a forma como trabalhamos, nos relacionamos e consumimos.	compartilhado	médio	provável	Investimentos em P&D, atualizações constantes da solução.
Concorrência de novas ferramentas	A concorrência de novas ferramentas refere-se à **disputa no mercado que surge com o advento de novas tecnologias e soluções, que desafiam as empresas e métodos existentes**. Essas novas ferramentas podem vir de qualquer direção e, muitas vezes, de onde menos se espera, redefinindo o cenário competitivo de um setor.	compartilhado	alto	provável	Análise competitiva, inovação contínua e diferenciação do produto.
Capacidade de atendimento	Capacidade de atendimento é o **volume máximo de solicitações que uma equipe ou serviço pode processar em um determinado período, sem comprometer a qualidade do atendimento**. Esse conceito envolve não apenas a quantidade de atendimentos, mas também a eficácia na resolução de problemas e a experiência geral do cliente. É a ponte entre o que a equipe pode entregar e o que a demanda dos clientes exige, sendo essencial para o sucesso e a sustentabilidade de um negócio.	compartilhado	médio	ocasional	Planejamento de recursos humanos, treinamento e contratação estratégica.
Reputação e conformidade legal	**Conformidade legal** refere-se ao potencial de perdas devido ao **não cumprimento de leis e regulamentos**, enquanto o **risco de reputação** diz respeito aos danos à **imagem e credibilidade** de uma organização, que muitas vezes são causados por falhas de conformidade.	compartilhado	médio	remota	Programas de compliance, auditorias regulares, transparência nas operações.
Mudanças na Legislação Tributária	Do ponto de vista dos riscos, as **mudanças na legislação** representam os potenciais problemas decorrentes da falha em **cumprir novas leis, regulamentos e normas** que afetam as operações de uma empresa. Esse tipo de risco é classificado como **risco legal, regulatório ou de conformidade**.	compartilhado	alto	ocasional	Revisão entre as partes, com recomposição do reequilíbrio econômico-financeiro do contrato.
Flutuações econômicas	Flutuações econômicas são os ciclos de altos e baixos na atividade econômica de um país, caracterizados por períodos de expansão (crescimento) e recessão (contração). Essas oscilações podem afetar a renda nacional, o emprego, a produção e os preços, e são causadas por fatores variados, como mudanças na oferta e demanda, custos de produção, políticas governamentais e o mercado financeiro.	compartilhado	alto	provável	Estratégias de mitigação de riscos financeiros
Dependência tecnológica	**Dependência tecnológica** refere-se a: **Integração de sistemas**: Se diferentes fornecedores fornecem câmeras, softwares de análise, armazenamento e redes, qualquer falha ou incompatibilidade pode comprometer todo o ecossistema. **Risco de lock-in**: Dependência de tecnologias proprietárias pode dificultar substituições ou atualizações, aumentando custos e reduzindo flexibilidade. **Escalabilidade e manutenção**: Em projetos nacionais, a interoperabilidade é crítica. Se uma empresa não acompanha atualizações ou sai do mercado, isso pode gerar grandes problemas. **Segurança cibernética**: Vulnerabilidades em um fornecedor podem afetar toda a cadeia, ampliando riscos de invasão ou vazamento de dados.	compartilhado	alto	ocasional	Diversificação de tecnologias e fornecedores, planos de contingência.
Questões de Segurança Cibernética	**Questões de segurança cibernética** referem-se a **potenciais ameaças e vulnerabilidades** que podem ser exploradas para causar danos, interrupções ou acesso não autorizado a sistemas e dados digitais. O foco está na probabilidade de um evento adverso ocorrer e no impacto potencial que ele teria sobre a confidencialidade, integridade e disponibilidade das informações. Conjunto de práticas, processos e tecnologias voltados para proteger sistemas, redes e dados contra acessos não autorizados, ataques, danos ou interrupções, garantindo **confidencialidade, integridade e disponibilidade** das informações.	compartilhados	alto	ocasional	Investimento em segurança cibernética, protocolos robustos de proteção de dados.
Mudança nas necessidades do cliente	**Mudanças nas necessidades do cliente** referem-se à ameaça de que os produtos ou serviços de uma empresa se tornem **obsoletos ou menos atrativos** devido à evolução das expectativas, hábitos ou prioridades dos consumidores. Isso pode impactar negativamente o desempenho financeiro, a participação de mercado e a reputação da marca.	compartilhado	alto	ocasional	Pesquisa de mercado e flexibilidade para adaptar os serviços.
Sinistralidade de câmeras, instalações e dispositivos de campo	**A exposição a defeitos de funcionamento e operacionais causados por vandalismo, depredação, ação com propósitos escusos e destruição proposital.**	Parceiros	alto	alta	Pesquisas da taxa de sinistralidade em operações similares. Atuação de mitigação da ação depredatória. Uso de tecnologia e instrumental de proteção aos ativos.

ANEXO D – CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES SIGILOSAS

1. Finalidade e Abrangência

1.1. O presente Anexo estabelece os critérios, procedimentos, controles e níveis de classificação das Informações Sigilosas e Informações Sensíveis tratadas no âmbito da Oportunidade de Negócio SMARTSAMPA, Confidencialidade e Informações Sigilosas deste Contrato.

1.2. Este Anexo aplica-se a toda e qualquer informação:

I – técnica, operacional, institucional, estratégica ou comercial;
II – decorrente de atividades da ON;
III – compartilhada entre as PARCEIRAS;
IV – produzida por qualquer PARCEIRA na execução da ON;
V – oriunda de órgãos da Administração Pública Municipal.

1.3. A classificação aqui prevista não se aplica a Dados Pessoais, cujo tratamento é regido exclusivamente pela Cláusula 8 e pelo Anexo A – Tratamento de Dados Pessoais.

2. Definições Complementares

2.1. Informação: qualquer dado, artefato, documento, registro, arquivo, código, rotina, relatório, metadado, log, estrutura lógica, modelo ou especificação relacionado à ON.

2.2. Autoridade Classificadora: órgão ou profissional designado pela governança da ON para classificar, revisar e reclassificar informações.

2.3. Sistema Crítico: componente tecnológico cuja indisponibilidade, violação ou modificação possa comprometer a continuidade operacional da ON ou serviços municipais.

2.4. Incidente de Segurança de Informação: qualquer evento que resulte ou possa resultar em acesso, uso, alteração, destruição, divulgação ou perda de informação classificada.

2.5. Cadeia de Custódia da Informação: conjunto de registros que permitem rastrear quem acessou, alterou, transportou, analisou ou descarregou determinada informação classificada.

3. Níveis de Classificação da Informação

As Informações tratadas no âmbito da ON serão classificadas em um dos seguintes níveis:

3.1. Nível 1 – PÚBLICA

Informações destinadas à divulgação ampla, cujo acesso não acarreta risco à segurança municipal, à operação da ON ou aos interesses das PARCEIRAS.

Exemplos:

informações publicadas em portais oficiais;

manuais públicos;

material promocional autorizado.

3.2. Nível 2 – RESTRITA

Informações cujo acesso indevido pode gerar risco operacional moderado, prejuízo institucional ou comprometer processos internos.

Exemplos:

atas de reuniões da governança;

relatórios de avanço da ON;

especificações de módulos não sensíveis;

documentação de APIs não críticas.

Regras principais:

acesso mediante autorização;

proibida cópia para dispositivos pessoais;

armazenamento em ambientes controlados.

3.3. Nível 3 – CONFIDENCIAL

Informações cujo acesso indevido pode causar prejuízo relevante, afetar negociações,

comprometer a segurança tecnológica da solução ou gerar impacto jurídico/institucional.

Exemplos:

diagramas internos da arquitetura;

documentação de integrações com sistemas legados;

regras de negócio sensíveis;

dados territoriais que possam revelar vulnerabilidades de serviços públicos.

Regras principais:

acesso apenas para equipes designadas;

obrigatoriedade de criptografia em repouso e trânsito;

registro em cadeia de custódia.

3.4. Nível 4 – ALTAMENTE CONFIDENCIAL / CRÍTICA

Informações estratégicas cujo acesso indevido pode causar:

risco à segurança urbana;

paralisação de serviços essenciais;

violação de sistemas críticos;

impactos severos à Administração Pública e às PARCEIRAS.

Exemplos:

chaves criptográficas mestras;

diagramas de segurança;

credenciais privilegiadas;

mapas de infraestrutura crítica;

lógica interna de módulos sensíveis do SMARTSAMPA.

Regras principais:

acesso restrito e nominal;

dupla autenticação e criptografia forte;

vedação de transporte fora do ambiente institucional;

políticas de segregação rígida;

monitoramento contínuo.

4. Procedimentos de Classificação

4.1. Toda informação criada, recebida ou modificada no âmbito da ON deverá ser avaliada quanto ao nível de classificação, de acordo com:

I – sensibilidade;
II – criticidade tecnológica;
III – impacto à política pública;
IV – risco jurídico ou reputacional;
V – potencial de exploração externa.

4.2. A classificação será feita pela Autoridade Classificadora, podendo ser revista pela governança da ON.

4.3. É obrigatória a aplicação de identificadores visuais, digitais e metadados que indiquem o nível de classificação da informação.

5. Acesso a Informações Classificadas

5.1. O acesso obedecerá aos critérios de:

I – “need to know”;
II – aprovação formal da governança;
III – trilhas de auditoria;
IV – mecanismos de autenticação forte.

5.2. Todos os acessos deverão ser registrados, permitindo rastreabilidade completa.

5.3. O compartilhamento externo exigirá:

a) justificativa formal;
b) registro em cadeia de custódia;
c) termo de confidencialidade;
d) criptografia ponta a ponta.

6. Armazenamento e Transporte

6.1. Informações classificadas devem ser armazenadas exclusivamente em:

I – ambientes institucionais aprovados;
II – infraestruturas gerenciadas conforme a Cláusula 8;
III – sistemas controlados pela governança da ON.

6.2. Proibições expressas:

uso de dispositivos pessoais;

envio por e-mail não institucional;

armazenamento em serviços de nuvem não autorizados;

transporte em mídias físicas sem autorização.

6.3. O transporte físico ou digital de informação classificada deve sempre:

ser criptografado;

ter registro de origem e destino;

ser realizado por pessoa autorizada.

7. Retenção, Conservação e Descarte

7.1. Os prazos de retenção serão definidos:

I – pelo PNO;
II – por exigência legal;
III – por deliberação da governança;
IV – por criticidade do módulo da solução.

7.2. O descarte seguro deve incluir:

sobrescrita;

destruição física controlada;

logs de eliminação;

relatório de auditoria.

8. Incidentes de Segurança Relacionados a Informações Classificadas

8.1. Qualquer incidente envolvendo informação classificada deve ser comunicado:

I – imediatamente;
II – com nível detalhado de impacto;
III – com descrição da informação afetada;
IV – com plano de mitigação.

8.2. Incidentes envolvendo Informação Altamente Confidencial são considerados críticos e exigem:

a) acionamento emergencial da governança;
b) comunicação à alta administração (quando aplicável);
c) relatório circunstanciado;
d) revisão de controles.

9. Auditoria e Monitoramento

9.1. A governança da ON poderá realizar auditorias:

I – periódicas;
II – extraordinárias;
III – temáticas (arquitetura, credenciais, acessos, logs).

9.2. As PARCEIRAS devem possibilitar o acesso a:

a) registros de acesso;
b) cadeia de custódia;
c) relatórios de incidentes;
d) evidências de conformidade.

10. Responsabilidades Específicas das PARCEIRAS

10.1. PRODAM deverá fornecer diretrizes, requisitos e padrões de segurança aplicáveis à ON.

10.2. A PARCEIRA deverá:

I – adotar medidas compatíveis com a criticidade da informação;
II – segregar ambientes;
III – manter controles de identidade e acesso;
IV – atender às normas internas da PRODAM.

11. Atualização e Evolução do Anexo

11.1. Este Anexo poderá ser atualizado:

I – por deliberação da governança da ON;
II – mediante alteração tecnológica significativa;
III – por mudança no ciclo de vida do SMARTSAMPA;
IV – por demanda de órgãos de controle ou normativos internos.

11.2. Versões atualizadas substituem automaticamente as anteriores, desde que registradas no processo administrativo da ON.

1.1. O presente Anexo detalha as obrigações operacionais, procedimentos, controles e instrumentos necessários para o adequado tratamento de Dados Pessoais e Dados Pessoais Sensíveis no âmbito da Oportunidade de Negócio SMARTSAMPA, em complemento direto à Cláusula 8 – Proteção de Dados e Segurança da Informação deste Contrato.

1.2. Este Anexo deve ser interpretado como extensão técnica da Cláusula 8, não criando regimes paralelos, mas especificando como tais obrigações serão executadas, documentadas e auditadas.

2. Papéis e Responsabilidades:

2.1. As PARCEIRAS reconhecem que os papéis de Controlador, Operador e Suboperador serão definidos caso a caso, conforme já previsto na Cláusula 8, especialmente em seu item 8.3, respeitando:

I – a finalidade do tratamento;
II – o ente responsável pela política pública ou serviço;
III – o instrumento jurídico firmado com o Cliente;
IV – os fluxos descritos no PNO.

2.2. Para fins operacionais, fica estabelecido que:

a) quando o tratamento decorrer de política pública municipal, o órgão público é, em regra, o Controlador;
b) a PRODAM atuará preferencialmente como Operadora;
c) a PARCEIRA atuará como Operadora ou Suboperadora, conforme o fluxo documental aprovado pela governança.

2.3. A definição final dos papéis será sempre registrada:

I – no PNO;
II – no contrato específico com Clientes (quando houver);
III – no processo administrativo da ON.

3. Categorias de Dados e Finalidades:
3.1. As categorias de dados tratadas no âmbito da SMARTSAMPA serão aquelas estritamente necessárias para:

I – execução de políticas públicas relacionadas ao território, mobilidade, eventos urbanos, atendimento digital e demais serviços integrados;
II – operação do ecossistema digital SMARTSAMPA;
III – funcionalidades previstas no PNO ou instrumento correlato.

3.2. Cada fluxo relevante de dados deverá conter:

a) descrição da categoria de dados pessoais tratada;
b) finalidade específica;
c) base legal aplicável (item 8.4 da Cláusula 8);
d) indicação do operador responsável;
e) prazo de retenção;
f) critérios de eliminação ou anonimização.

3.3. O registro desses fluxos ocorrerá nos mapas de tratamento da ON e ficará disponível para consulta pela governança.

4. Bases Legais:

4.1. As bases legais previstas no item 8.4 da Cláusula 8 serão aplicadas conforme cada operação, devendo constar nos documentos:

I – PNO (versão vigente);
II – Plano de Governança;
III – instrumentos firmados com Clientes.

4.2. A mudança de base legal motivada por alteração de finalidade deverá ser previamente submetida à governança da ON.

5. Direitos dos Titulares (Complemento ao item 8.5)

5.1. Em cumprimento ao item 8.5 da Cláusula 8, cada PARCEIRA deverá manter mecanismos para atender, de forma rastreável, solicitações de titulares relativas a confirmação de tratamento, acesso, correção, anonimização, revogação de consentimento (quando aplicável), informação sobre compartilhamento, portabilidade (quando cabível).

5.2. O ponto de contato principal com o titular será o órgão público Controlador.
PRODAM e PARCEIRA prestarão suporte operacional mediante procedimentos definidos no PNO.

6. Compartilhamento de Dados:

6.1. Como complemento ao item 8.6, todo compartilhamento de dados pessoais com terceiros deverá:

I – ter base legal válida;
II – ser documentado no processo administrativo;
III – ser amparado por cláusulas contratuais equivalentes às deste Anexo e da Cláusula 8;
IV – estar previsto no PNO ou instrumento com o Cliente.

6.2. Operações que envolvam subcontratados exigem:

a) assinatura de Termo de Confidencialidade;
b) aceite das políticas de segurança da PRODAM;
c) aceite deste Anexo e da Cláusula 8.

7. Segurança da Informação:

7.1. Os controles previstos no item 8.7 serão detalhados operacionalmente:

I – no Plano de Governança da ON;
II – nos controles de acesso à solução SMARTSAMPA;
III – nos procedimentos de criptografia, autenticação, segregação e rastreabilidade;
IV – nos requisitos de proteção de dados territoriais e urbanos sensíveis.

7.2. A PARCEIRA compromete-se a implementar controles compatíveis com:

a) normas internas de segurança da PRODAM;
b) políticas de classificação de informação;
c) requisitos específicos do módulo da solução.

8. Incidentes de Segurança:

8.1. Incidentes descritos no item 8.8 deverão ser comunicados por escrito à outra PARCEIRA:

I – imediatamente, em até 24 horas após a ciência;
II – com informações suficientes para avaliação preliminar;
III – com atualização contínua até o encerramento do incidente.

8.2. A governança da ON será responsável por:

a) qualificar o impacto;
b) indicar medidas de mitigação;
c) decidir sobre comunicações obrigatórias à ANPD e titulares;
d) registrar todo o fluxo no processo administrativo.

9. Retenção e Eliminação de Dados:

9.1. Os prazos de retenção definidos no item 8.9 serão detalhados conforme:

I – contrato com Cliente;
II – legislação aplicável à política pública correlata;
III – requisitos do módulo da solução.

9.2. A eliminação ou anonimização deve:

a) ocorrer de forma segura;
b) ser documentada;
c) ser aprovada pela governança.

10. Transferência Internacional de Dados:

10.1. Qualquer operação tratada no item 8.10 exigirá:

I – avaliação de risco;
II – cláusulas contratuais específicas;
III – garantia de nível adequado de proteção;
IV – registro formal no processo administrativo da ON.

11. Encarregado (DPO) e Comunicação:

11.1. PRODAM e PARCEIRA deverão manter seus Encarregados atualizados no processo administrativo da ON.

11.2. As comunicações relacionadas a direitos de titulares, incidentes e avaliações de risco ocorrerão:

I – preferencialmente pelo SEI;
II – por e-mail institucional, quando necessário;
III – com rastreabilidade garantida.

12. Atualizações:
12.1. As atualizações previstas no item 8.12 serão incorporadas mediante:

I – deliberação da governança;
II – termo aditivo, quando necessário;
III – registro no processo da ON;
IV – comunicação às áreas técnicas envolvidas.

ANEXO E - - Relatório de Impacto à Proteção de Dados Pessoais

O presente anexo traz explicações a respeito da utilização da tecnologia no Programa Smart Sampa de forma detalhada com o intuito de tranquilizar, esclarecer e informar com relação a segurança, privacidade e utilização da tecnologia para monitoramento que deverá estar disponível na nova plataforma. Entendendo ser necessário demonstrar a utilização da Plataforma Smart Sampa e o compromisso com a população garantindo o compliance com a legislação vigente e interesse público afastando qualquer dúvida quanto à Implantação e Utilização da Plataforma Smart Sampa como parte das políticas de públicas de integração, cooperação, interoperabilidade dos serviços Municipais e de Governo Digital.

1. Análise de riscos à Proteção de Dados Pessoais

Este relatório de impacto à proteção de dados pessoais tem como objetivo avaliar os riscos e identificar as medidas necessárias para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) no contexto de um sistema de videomonitoramento com inteligência artificial embarcada e reconhecimento facial implementado por órgão público no âmbito da segurança pública.

1.1. Identificação dos dados pessoais coletados e armazenados

O sistema de videomonitoramento com inteligência artificial embarcada e reconhecimento facial coleta e armazena os seguintes dados pessoais: (i) Imagens de vídeo com reconhecimento facial; (ii) Data e hora da coleta das imagens. Esses dados são coletados para fins de segurança pública e são armazenados em servidores do órgão público responsável pelo sistema.

1.2. Avaliação dos riscos

Em seguida, avaliamos os riscos envolvidos na coleta e armazenamento desses dados pessoais. Identificamos os seguintes riscos: (i) possibilidade de coleta de dados pessoais sem o consentimento dos indivíduos; (ii) uso indevido dos dados pessoais coletados; (iii) falhas de segurança que permitam acesso não autorizado às imagens coletadas; (iv) possibilidade de discriminação ou preconceito no reconhecimento facial; (v) falta de transparência no uso dos dados coletados; (vi) possibilidade de vazamento de dados pessoais.

1.3. Medidas de proteção dos dados pessoais

Para mitigar os riscos identificados, a PARCEIRA implementará as seguintes medidas de proteção dos dados pessoais, considerando normas ISO relevantes:

(i) Coleta de dados pessoais apenas para fins específicos e legítimos relacionados à segurança pública, em conformidade com a LGPD (13.709/2018) e ISO 27701:2019 - Privacidade da Informação - Extensão à ISO/IEC 27001 e ISO/IEC 27002;

(ii) Obtenção de consentimento dos indivíduos em caso de coleta de dados pessoais sensíveis, de acordo com a ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais, seguindo a LGPD (13.709/2018) e as exceções nela descritas para fins de segurança pública;

(iii) Utilização de criptografia para proteção dos dados pessoais armazenados, seguindo as recomendações da ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;

(iv) Implementação de políticas de segurança da informação para prevenção de acessos não autorizados e monitoramento constante da rede e sistemas, em conformidade com a ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos;

(v) Restrição de acesso aos dados pessoais apenas aos funcionários autorizados e treinados sobre a importância da proteção de dados pessoais, seguindo as recomendações da ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;

(vi) Transparência no uso dos dados coletados e disponibilização de informações claras sobre a finalidade do sistema de monitoramento, em conformidade com a ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais;

(vii) Implementação de um processo de avaliação de impacto à proteção de dados pessoais em conformidade com a ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança - Técnicas para a Avaliação de Privacidade e Impacto à Proteção de Dados.

1.4. Conclusão

A implementação de um sistema de vídeo monitoramento com inteligência artificial embarcada e reconhecimento facial por órgão público no âmbito da segurança pública envolve riscos significativos à proteção de dados pessoais. No entanto,

medidas de proteção podem ser implementadas para mitigar esses riscos, garantindo a conformidade com a LGPD e normas ISO relevantes.

É importante destacar a importância da transparência no uso desses dados e a necessidade de se garantir que os indivíduos sejam informados sobre a coleta e o processamento de seus dados pessoais. Além disso, é fundamental que o órgão público responsável pelo sistema de videomonitoramento esteja preparado para lidar com possíveis incidentes de segurança da informação, bem como com as solicitações de acesso e correção de dados pessoais pelos indivíduos afetados.

Referências Normativas:

(i) ISO 27701:2019 - Privacidade da Informação - Extensão à ISO/IEC 27001 e ISO/IEC 27002;
(ii) ISO/IEC 29100:2011 - Tecnologias da Informação - Privacidade e Proteção de Dados Pessoais - Estrutura e Princípios Gerais;
(iii) ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação;
(iv) ISO/IEC 27001:2013 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos;
(v) ISO/IEC 29134:2017 - Tecnologia da Informação - Técnicas de Segurança - Técnicas para a Avaliação de Privacidade e Impacto à Proteção de Dados.

2. Matriz de Risco a Proteção de Dados

	Probabilidade Alta	**Probabilidade Média**	**Probabilidade Baixa**
Impacto Alto	Acesso não autorizado a dados pessoais (Risco Médio)	Uso indevido de dados pessoais (Risco Médio)	Violação da privacidade de indivíduos (Risco Médio)
	Falhas de segurança que permitem o acesso não autorizado a dados pessoais (Risco Alto)	Falhas no reconhecimento facial que podem levar à identificação	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Baixo)

		equivocada de indivíduos (Risco Médio)	
Impacto Médio	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Médio)	Violação da privacidade de indivíduos (Risco Médio)	Uso indevido de dados pessoais (Risco Baixo)
	Falhas de segurança que permitem o acesso não autorizado a dados pessoais (Risco Médio)	Falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos (Risco Baixo)	-
Impacto Baixo	Interrupção ou indisponibilidade do sistema de videomonitoramento (Risco Baixo)	-	-

A probabilidade de cada risco ser alto, médio ou baixo foi determinada com base na avaliação dos controles existentes para mitigar o risco, bem como a frequência e impacto de incidentes anteriores similares.

A seguir, são fornecidas mais informações sobre cada risco e as medidas de proteção recomendadas para mitigá-los:

2.1. Acesso não autorizado a dados pessoais

(i) Probabilidade alta: Existe um alto risco de acesso não autorizado a dados pessoais devido a falhas de segurança no sistema de vídeo monitoramento.

(ii) Probabilidade média: Existe uma probabilidade média de acesso não autorizado a dados pessoais.

(iii) Probabilidade baixa: A probabilidade de acesso não autorizado a dados pessoais é baixa devido à presença de medidas de segurança adequadas, como autenticação forte e controles de acesso.

2.1.1. Medidas de proteção recomendadas:

(i) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.
(ii) Uso de autenticação forte, como autenticação de dois fatores, para impedir que pessoas não autorizadas acessem o sistema.
(iii) Implementação de criptografia de dados para garantir que os dados pessoais permaneçam seguros, mesmo se houver acesso não autorizado.

2.2. Uso indevido de dados pessoais

(i) Probabilidade alta: Existe um alto risco de uso indevido de dados pessoais devido a possíveis falhas no treinamento da inteligência artificial e do reconhecimento facial.
(ii) Probabilidade média: Existe uma probabilidade média de uso indevido de dados pessoais.
(iii) Probabilidade baixa: A probabilidade de uso indevido de dados pessoais é baixa devido à existência de políticas e procedimentos adequados para garantir o uso adequado dos dados.

2.2.1. Medidas de proteção recomendadas:

(i) Implementação de políticas e procedimentos claros para garantir que os dados pessoais sejam usados apenas para fins legítimos e autorizados.
(ii) Treinamento adequado de pessoal para garantir que os dados pessoais sejam manuseados de acordo com as políticas e procedimentos estabelecidos.
(iii) Implementação de auditorias regulares para garantir que o uso de dados pessoais esteja em conformidade com as políticas e procedimentos estabelecidos.

2.3. Violação da privacidade de indivíduos

(i) Probabilidade alta: Existe um alto risco de violação da privacidade de indivíduos devido a falhas de segurança no sistema de vídeo monitoramento.

(ii) Probabilidade média: Existe uma probabilidade média de violação da privacidade de indivíduos.

(iii) Probabilidade baixa: A probabilidade de violação da privacidade de indivíduos é baixa devido à existência de medidas de proteção adequadas, como criptografia de dados e controles de acesso.

2.3.1. Medidas de proteção recomendadas:

(i) Implementação de políticas e procedimentos claros para garantir que a privacidade dos indivíduos seja respeitada.

(ii) Uso de criptografia de dados para garantir que os dados pessoais permaneçam seguros.

(iii) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.

2.4. Falhas de segurança que permitem o acesso não autorizado a dados pessoais.

(i) Probabilidade alta: Existe um alto risco de falhas de segurança que permitam o acesso não autorizado a dados pessoais.

(ii) Probabilidade média: Existe uma probabilidade média de falhas de segurança que permitam o acesso não autorizado a dados pessoais.

(iii) Probabilidade baixa: A probabilidade de falhas de segurança que permitam o acesso não autorizado a dados pessoais é baixa devido à existência de medidas de proteção adequadas.

2.4.1. Medidas de proteção recomendadas:

(i) Implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais.

(ii) Uso de autenticação forte para impedir que pessoas não autorizadas acessem o sistema.

(iii) Implementação de criptografia de dados para garantir que os dados pessoais permaneçam seguros.

2.5. Falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos

(i) Probabilidade alta: Existe um alto risco de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos.

(ii) Probabilidade média: Existe uma probabilidade média de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos.

(iii) Probabilidade baixa: A probabilidade de falhas no reconhecimento facial que podem levar à identificação equivocada de indivíduos é baixa devido à existência de medidas de proteção adequadas.

2.5.1. Medidas de proteção recomendadas:

(i) Implementação de testes regulares para garantir a precisão do reconhecimento facial.

(ii) Treinamento adequado da inteligência artificial para garantir a precisão do reconhecimento facial.

(iii) Implementação de políticas e procedimentos claros para lidar com casos em que a identificação equivocada de indivíduos ocorra.

2.6. Com base na matriz de risco, é recomendado que medidas de proteção adequadas sejam implementadas para mitigar os riscos identificados. Essas medidas incluem a implementação de políticas e procedimentos claros para garantir que os dados pessoais sejam usados apenas para fins legítimos e autorizados, o treinamento adequado de pessoal para lidar com dados pessoais, a implementação de auditorias regulares para garantir a conformidade com as políticas e procedimentos estabelecidos, o uso de criptografia de dados para garantir que os dados pessoais permaneçam seguros, a implementação de controles de acesso para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais e a implementação de testes regulares para garantir a precisão do reconhecimento facial.

2.7. Essas medidas de proteção devem ser baseadas nas normas ISO 27001 e ISO 27701, que fornecem orientações sobre a implementação de um sistema de gestão de segurança da informação e um sistema de gestão de privacidade de informações pessoais, respectivamente. Essas normas ajudam a garantir que as medidas de proteção implementadas sejam adequadas e eficazes.

2.8. Além disso, é importante que uma avaliação de impacto à proteção de dados seja realizada regularmente para garantir que o sistema de videomonitoramento continue a ser compatível com as normas de proteção de dados pessoais e para identificar novos riscos à privacidade dos indivíduos.

3. Compliance e das Garantias

3.1 Necessidades e Garantias

A necessidade de assegurar as garantias básicas a direitos fundamentais, por ela afetados e suas normas correspondentes – em especial, os direitos de imagem, de privacidade e de proteção de dados pessoais, desta forma além de já prever mecanismos para garantir estes direitos, o programa é plenamente aderente a possíveis regulações posteriores pela ANPD (Agência Nacional de Proteção de Dados), podendo se adequar a novos processos, fluxos e tecnologias de proteção de dados e privacidade.

3.2 Dados Armazenados e Privacidade

A utilização da solução deve seguir as diretrizes e finalidades do Programa Smart Sampa, sendo vedada qualquer utilização fora do escopo aprovado, garantindo a privacidade e proteção dos dados pessoais. Os controles de acessos e privilégios de usuário devem impedir qualquer acesso ou uso fora do especificado, considerado invasivo/desnecessário a atividade e escopo do Programa Smart Sampa. Todo dado armazenado deve ser criptografado e dados que não são de interesse do poder público, sem requisição de qualquer órgão será eliminada em 30 dias, incluindo as imagens e dados biométricos limitando o volume de dados armazenados. Qualquer imagem, dado ou informação, só poderá sair do sistema, ser enviada ou cedida mediante solicitação oficial de órgão competente conforme legislação vigente, não sendo divulgada, veiculada ou utilizada para qualquer outro fim além dos previstos legalmente. Evitando assim a exposição desnecessária de pessoas e a invasão à privacidade, tendo em vista que a finalidade das imagens e dados captados não é a invasão à privacidade, mas sim melhorar os serviços oferecidos e a segurança no Município.

3.3 Acompanhamento contínuo dos resultados

Deve ser monitorado durante o seu continuum, por meio de uma Avaliação de Resultado da implementação, assim como das políticas públicas suportadas pelo programa, a fim de avaliar os resultados de seu objetivo e a correspondência entre as análises prévias sobre o impacto e seus efeitos com a realidade concretamente observada e documentada. Conforme já definido, toda e qualquer projeto passará regularmente a cada 6 meses por revisões, sendo analisado todos os impactos, eficiência e alinhamento, com as

expectativas prévias sendo todo o processo documentado, incluindo todos os ajustes de processos e procedimentos realizados pelos agentes. Qualquer variação de resultado positivo ou negativo será possível corrigir, como qualquer intercorrência, que incline o programa em direção diferente da definida como referência. Sendo um processo de melhoria constante dos sistemas que compõem a Plataforma, assim como tudo que compõem o Programa Smart Sampa, com metodologias tais como PDCA, six sigma, 5S, BSC, entre outros utilizados para fazer a gestão e revisões constantes, em todos os aspectos do programa, incluindo a solução tecnológica adotada para garantir o alinhamento da tecnologia aos interesses públicos, sendo todos os resultados avaliados e publicados no portal da transparência e demais canais a cada ciclo.

3.3.1. Tratamento de Dados

Deve ser pública a descrição do contexto, da natureza, do escopo, da necessidade e da finalidade do tratamento das categorias de dados pessoais (art. 5º, inc. I, LGPD) e de dados pessoais sensíveis (art. 5º, inc. II, LGPD), envolvidas no Programa disponibilizadas através do portal da transparência e demais canais da Prefeitura Municipal de São Paulo, deixando clara a forma como os dados serão captados, tratados, processados, armazenados e eliminados, com exemplos claros da utilização e simplificando o entendimento do processo e utilização da tecnologia. Exemplo de dados utilizados: (i) dados de Atendimento; (ii) dados de Identificação; (iii) Dados Biométricos (iv) Características; (v) Contextos e Ações; (vi) Dados e Documentos relacionados

3.3.2. Segurança do Programa Smart Sampa

Será instituído como padrão nos serviços, integrações, cooperações e qualquer outra atividade ligada direta ou indiretamente ao Programa Smart Sampa, os parâmetros definidos a partir dos documentos abaixo:

(i) Estrutura Organizacional
(ii) Política de Segurança da Informação
(iii) Política de Segurança Cibernética
(iv) Política de Transparência e Compliance
(v) Política de Privacidade (Usuários finais)
(vi) Política de Proteção de Dados e Privacidade (Uso Interno)
(vii) Política de Integridade e ética
(viii) Padrões, Processos e Procedimentos operacionais

(ix) Mapa de Riscos e Impactos
(x) Relatório de Impacto à Proteção de dados pessoais
(xi) Categorização dos dados, informações e ciclo de vida
(xii) Plano de Gestão das Hipóteses de Tratamento de dados pessoais
(xiii) Plano de Mitigação de Riscos
(xiv) Plano de Resposta a Incidentes
(xv) Plano de Recuperação de Desastres
(xvi) Plano de Contingência

Estes documentos devem ser desenvolvidos em conjunto, mas especialmente da PARCERIA, tendo em vista às variações de tecnologia e processos que serão adotados, sendo assim necessário alinhamento. Não sendo possível defini-los sem o entendimento entre o provedor de serviços (PARCERIA) e operador (PRODAM). O desenvolvimento desses documentos é necessário para estabelecer as normas e processos para a operação da plataforma no dia a dia e previsão e prevenção de eventuais eventos adversos.

Esses documentos serão elaborados logo após a instalação do projeto, após 3 meses da assinatura do contrato, trazendo assim maior efetividade na segurança e transparência do Programa Smart Sampa como um todo

4. Utilização da Plataforma e Tratamento de Dados

4.1 Apenas órgãos do poder público contratante poderão operar a Plataforma Smart Sampa, tendo acesso aos seus dados e processos. A PARCEIRA não terá acesso a dados sensíveis ou sigilosos. Em casos excepcionais onde exista a necessidade de acesso durante a implementação, o conselho de gestão da plataforma irá deliberar sobre a autorização dos envolvidos, que deverão assinar termo de sigilo e confidencialidade, desenvolvido especificamente para a atividade desempenhada, devendo estes estar sempre acompanhados de um fiscal da PRODAM durante toda a implementação.

4.2. Tão logo os documentos desse RIPD estejam prontos e aprovados, serão encaminhados para conhecimento do encarregado de dados e do controle interno do órgão público.

4.3. Será observado o compartilhamento de dados com propósitos legítimos, específicos e explícitos, limitando ao mínimo necessário para o atendimento das finalidades do programa. Em observância ao o julgamento conjunto da Ação Direta de Inconstitucionalidade nº 6.649/DF e da Arguição de Descumprimento de Preceito Fundamental nº 695/DF.

4.4. O compartilhamento de informações pessoais em atividades de inteligência, observará adoção de medidas estritamente necessárias ao atendimento do interesse público, podendo ter acompanhamento do poder judiciário, com estrito controle de acesso.

4.5. Do registro das operações

A Plataforma deverá manter o registro das operações de tratamento de dados pessoais realizadas. Para cumprir com esta obrigação, esta etapa objetiva identificar os processos do tratamento de dados pessoais, os fluxos e ciclos de vida desses dados dentro e fora do programa (informações acessadas, coletadas, usadas, transferidas, armazenadas ou compartilhadas), em conformidade ao artigo 37 da LGPD.

4.5.1. Os controladores e operadores realizarão e manterão o registro das operações com a devida associação das bases legais, em especial quando for o legítimo interesse, desta forma poderá ser solicitado pela autoridade nacional de proteção de dados (ANPD).

4.5.2. Todos os processos e atividades desenvolvidas ou relacionadas ao Programa Smart Sampa, serão documentadas com o intuito de trazer garantias e demonstrar a efetividade da governança adotada, em privacidade, transparência, boas práticas, processos, códigos de condutas e todas as outras medidas para o cumprimento da legislação.

4.5.3. Desta forma todo o Programa Smart Sampa poderá ser auditado quando necessário, para demonstrar a efetividade das medidas adotadas, objetivos almejados e resultados obtidos. Mostrando de forma cronológica todas as alterações e adequações realizadas ao longo do Programa, para atender as regulamentações e legislação vigente, conforme LGPD em seus artigos 37, 38, 46, 47, 48, 49 e 50. Que exige controle, governança e transparência no processamento de dados, identificando a natureza, necessidade, objetivos e riscos do tratamento de dados realizado.

4.6. Canal de Comunicação

Será criado um canal de comunicação web site pelo Controlador órgão público ao CRM para atendimento aos titulares dos dados onde os usuários da plataforma poderão solicitar informações referentes ao tratamento dos seus dados pessoais e terão acessos aos controladores das informações, conforme dispõe os artigos 9º, 17º e 22º todos da Lei 13.709 de 14 de 08/2018 (LGPD) de

forma que os titulares dos dados possam esclarecer dúvidas e entender o processamento dos dados.

4.6.1. Terá a devida publicidade realizada em eventual site do programa e nos canais de comunicação do órgão público, bem como em peças publicitárias da municipalidade.

4.6.2. A plataforma Smart Sampa desde sua implementação deverá fornecer informações de operação que serão disponibilizadas no portal da transparência do órgão público, incluindo impacto e resultados.

4.6.3. O tratamento de dados de idosos deverá ser efetuado de maneira simples, clara, acessível e adequada ao seu entendimento. Garantindo a inclusão da terceira idade nas políticas públicas que utilizam tecnologia e tratamento de dados em seus processos, tendo pleno conhecimento da utilização da de seus dados e as hipóteses em que são processados e com qual objetivo. Garantindo igualdade de acesso e compreensão cumprindo o Estatuto do Idoso Lei nº 10.741, de 1º de outubro de 2003, e as diretrizes da Agência Nacional de Proteção de Dados Lei 13.853 de 2019, dando atenção especial ao disposto no Art. 55-J inciso XIX da Lei 13.853.

5. Compliance do Programa na utilização da tecnologia e processos adotados

O Chefe de Equipe de Fiscalização e Compliance da PARCEIRA deverá fornecer aos operadores e seus internos orientações sobre o tratamento de dados pessoais, além de garantir que todos os operadores possuam o devido treinamento para operação da plataforma e tratamento de dados. Fazendo requalificação de pessoal sempre que necessário.

5.1. O Chefe de Equipe de fiscalização e compliance ficará encarregado de fiscalizar os processos, a utilização da plataforma e o Compliance (fazer cumprir todas as políticas, normas, processos adotados e legislação vigente). Os processos e soluções adotados devem mitigar impactos aos direitos individuais e trazer garantias de privacidade, segurança e transparência, tornando a tecnologia menos invasiva na captura de dados e não deixando estas informações disponíveis aos operadores sem que exista necessidade. Devendo a utilização ser aprovada pelo Chefe de Equipe de Fiscalização e Compliance e mantendo todos os dados armazenados criptografados.

5.2 Para uso interno será instituída a Política de Proteção de Dados e Privacidade, trazendo as diretrizes sobre sigilo e privacidade, além de punições administrativas cabíveis, a desvios dos Servidores Públicos no ato de suas

funções. Dispondo sobre as práticas adotadas com relação à privacidade e à proteção de dados pessoais no âmbito do Programa, contendo todo o detalhamento necessário ao entendimento com exemplos do que é permitido e do que não é, conforme as melhores prática e legislação vigente.

5.3. No caso de criação de site vinculado ao projeto, atualmente, não é prevista a utilização de websites ou Cookies no programa voltados aos usuários finais (munícipes etc), devido aos vários canais utilizados para comunicação já existentes (portal da transparência, capital.sp.gov.br e outros endereços da PMSP). Em caso de futura implantação de websites e Cookies voltados ao programa, este seguirá toda a legislação vigente, incluindo aviso de Privacidade, política de privacidade, exibindo a notificação com a política de Cookies e rastreabilidade dos usuários entre outros mecanismos que visam garantir a privacidade dos usuários ao utilizar sites e aplicativos.

6. Parametrização dos Analiticos e Processos

6.1. Parâmetro para gerar alertas automáticos A plataforma só deve produzir alertas quando a análise dos analíticos for de maior ou igual a 90% de paridade. Todo e qualquer evento em que o analítico esteja menor a 90% será automaticamente descartado.

6.2. Todos os alertas gerados ficarão armazenados, para análise e revisão dos processos de tratamento e tomada de decisão, com o intuito de garantir eficiência e o aprimoramento do processo.

7. Da Utilização da Plataforma

7.1. A Plataforma Smart Sampa deve suportar a operação de forma eficiente, segura e transparente, seguindo a política de segurança da informação vigente, que será atualizada sempre que se mostre necessário. A solução deve manter histórico detalhado de tudo que ocorrer na plataforma, incluindo atividade dos operadores e agentes. Deve possuir sistema robusto de controle, níveis de acesso, permissões e privilégios. Sendo gerido de forma unificada servindo tanto para controle e acesso da plataforma, como para dar acesso aos espaços físicos dos centros (Centro Operacional e Centro Administrativo) que se fizerem necessários, onde o controle de acesso estará instalado.

DECLARAÇÃO DE TRANSAÇÃO COM PARTE RELACIONADA

A <**razão social**>, CNPJ nº <**cnpj**>, endereço <**endereço completo**>, neste ato representada por <**nome completo**>, <**nacionalidade**>, documento de identidade nº <**XXXX**>, órgão emissor <**XXXX**> , CPF nº <**XXXX**>, <**cargo/função**>, **DECLARA** sob as penas da lei, em atenção à Política de Transações com Partes Relacionadas da PRODAM e a fim de afastar situações que possam configurar conflito de interesses, que:

(_) não é parte relacionada e não possui em seu quadro de administradores, proprietários ou sócios, pessoa com influência significativa ou envolvida em decisão de interesse exclusivo da PRODAM.

(_) é parte relacionada e/ou possui em seu quadro de administradores, proprietários ou sócios, pessoa com influência significativa ou envolvida em decisão de interesse exclusivo da PRODAM.

Composição da Alta Administração (Presidente, Vice-Presidente, Diretores, Conselheiros de Administração, proprietários, sócios etc., conforme o caso):

Nome completo	CPF	Cargo / Função

Nada mais a declarar e ciente da responsabilidade administrativa, civil e penal pelas informações prestadas, firmo a presente declaração.

_____
(Local e Data)

_____
(Nome e assinatura do responsável)

DECLARAÇÃO

Declaramos, sob as penas da lei, que a empresa ....., CNPJ/MF nº ....., não está impedida de participar de licitações e de ser contratada pela **PRODAM**, por não estar enquadrada em nenhuma das hipóteses do art. 38, da Lei 13.303/16.

Declaramos, ainda, sob as penas da Lei, que não empregamos familiar de agente público que exerça cargo em comissão ou função de confiança na **PRODAM**.

_____
(Local e Data)

_____
(Nome e Assinatura do Declarante)