

EDITAL DE CHAMAMENTO PÚBLICO PARA SELEÇÃO DE PARCEIRO PRIVADO					
Edital Nº XXXXX/2025 - Objeto - SMART SAMPA PRODAM					
Item	Título	Descrição dos requisitos de qualificação técnica	Motivação/Finalidade	Forma de Demonstração	Critério de Aceitação
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.
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.
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.

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.
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.
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.
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.

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.
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.
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.
11	Suporte a APIs e Integrações Padronizadas	A plataforma deve disponibilizar APIs ou mecanismos equivalentes que permitam integração com sistemas legados e de terceiros.	Viabilizar interoperabilidade entre VMS, OMS, IA, segurança pública, CET, PM, Bombeiros etc.	Documentação de API, guia de integração, declaração do fabricante.	Apresentação de documentação oficial demonstrando suporte a APIs ou métodos de integração.

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.
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.
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.
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.

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.
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)
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.

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.
----	---	---	--	--	---

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.
----	---------------------------------------	--	---	--	--

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.
----	----------------------------	---	--	---	--

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, permitindo que dados críticos permaneçam disponíveis mesmo diante de interrupções pontuais. A plataforma deve assegurar replicação ou cópia segura dos dados entre componentes compatíveis, evitando perda de informações essenciais.	Garantir continuidade e integridade dos dados em caso de falhas	Documentação técnica, descrição do fluxo de tratamento de incidentes, arquitetura funcional do OMS, prints ou modelos de tela exemplificativos, declaração do fabricante	Comprovação documental de que a solução dispõe de mecanismos de registro, classificação e encaminhamento de incidentes, com fluxo rastreável e aderente ao processo operacional definido pela Administração.
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
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.

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 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.
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.
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 possuïrem.
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.

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.
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 externamente 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.
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.

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.
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.
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.

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.
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.
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.
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.

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.
----	---	---	--	---	---

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.
----	---------------------------------------	--	--	--	---

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.
----	---	---	---	---	--

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.
----	--	--	--	---	---

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.
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.
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.

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.
---	---	--	--	---

*** Exemplos de Evidências:**

- Documento Manual-Do-Fabricante.pdf, pág.13-17, plataforma de gerenciamento
- Documento AtestadoDeCapacidadeTecnica-XPTO.pdf, pág.3-4, arquitetura da solução
- Site h <https://solucaoXPTO.com/local/docs/sobre-gerenciamento>, texto e imagem do tópico ABCD
- Site h <https://solucaoXPTO.com/local/docs/sobre-gerenciamento>, video demonstrativo ABCD, dos 3min40seg aos 4min53seg - Video ControleDeAcesso.mp4, dos 3min40seg aos

%	Pontos	Critério de Qualificação Técnica
0–100%	Até 10 pts	Arquitetura Modular e Escalabilidade
0–100%	Até 10 pts	Segurança e Compliance (Exceto LGPD detalhada)
0–100%	Até 12 pts	Criptografia e Controle de Acesso
0–100%	Até 12 pts	Logs, Auditoria e Observabilidade
0–100%	Até 14 pts	IA e Analytics (Facial, OCR, Comportamento, Contagem, Forense)
0–100%	Até 10 pts	OMS — Orquestração de Incidentes e Despacho
0–100%	Até 10 pts	Interoperabilidade (APIs)
0–100%	Até 8 pts	Atualização Não Disruptiva e Versionamento
0–100%	Até 8 pts	Resiliência de Rede e Fallback Automático
0–100%	Até 6 pts	Isolamento Modular Multi-cliente
0–100%	Até 5 pts	Telemetria e Integridade dos Dispositivos
0–100%	Até 5 pts	Documentação Técnica e Manuais