

ESP-DIR.EDUC. PARA O TRANSITO E FISCALIZACAO

Estudo Técnico Preliminar 2/2026**1. Informações Básicas**

Número do processo: 140.01306393/2025-23

2. Descrição da necessidade

O DETRAN-SP necessita contratar serviços especializados para o desenvolvimento, modernização e implantação de soluções tecnológicas críticas, indispensáveis para assegurar a continuidade, a segurança, a estabilidade e a evolução de seu ecossistema digital. O conjunto atual de sistemas que suportam as atividades finalísticas e administrativas do órgão encontra-se em estágio de obsolescência, limitado por arquiteturas legadas, infraestrutura saturada e ausência de capacidades tecnológicas essenciais ao funcionamento moderno e seguro dos serviços públicos de trânsito.

A demanda envolve o desenvolvimento e evolução de quatro sistemas estruturantes — Prova Prática, Registro de Sinistro de Trânsito, Plataforma Estadual de Vistoria e Plataforma de Pagamentos — todos classificados como de alta criticidade, dada sua relação direta com atendimento ao cidadão, fiscalização, segurança viária, arrecadação e governança administrativa. Cada uma dessas soluções apresenta gargalos operacionais relevantes, como fragmentação de dados, limitações de conectividade, baixa rastreabilidade, ausência de cadeia de custódia digital, insuficiência de mecanismos de auditoria e incapacidade de processar grandes volumes de informações de maneira segura e padronizada.

A infraestrutura tecnológica atualmente utilizada, predominantemente baseada em ambiente on-premises, não dispõe de elasticidade, resiliência, escalabilidade ou capacidade de processamento compatíveis com os requisitos dessas plataformas. A ausência de redundância, a limitação de recursos computacionais, a incapacidade de suportar arquiteturas Cloud-Native e a falta de ferramentas modernas de orquestração, segurança e gestão de APIs representam risco real à continuidade dos serviços públicos, especialmente em cenários de alta demanda, como picos de atendimento, operações em campo e integração com sistemas externos.

Do ponto de vista operacional, destaca-se a necessidade de soluções capazes de operar de forma Offline-First, com sincronização automática e segura assim que houver conectividade, requisito crítico para atividades realizadas em campo, como registro de sinistros e provas práticas. A atual dependência de conectividade constante impossibilita a operação segura em áreas com sombra de rede, gera retrabalho, causa inconsistências e compromete a integridade de dados essenciais ao processo administrativo.

Outro fator determinante para a necessidade da contratação é a ausência de recursos tecnológicos adequados à auditoria, segurança e governança. As novas plataformas exigem imutabilidade de dados, trilhas de auditoria completas, criptografia avançada, mecanismos de detecção de fraude, validação geoespacial de alta precisão, autenticação robusta, monitoramento contínuo e proteção contra-ataques cibernéticos — elementos incompatíveis com o ambiente atual.

Do ponto de vista de gestão da informação, a fragmentação dos sistemas existentes impede a consolidação de uma fonte única da verdade, dificulta análises avançadas, limita a fiscalização em tempo real, inviabiliza o uso de inteligência de dados e aumenta o risco de inconsistências operacionais e financeiras. A modernização tecnológica é necessária para permitir governança centralizada, integração padronizada, processamento em larga escala e adoção de modelos de Inteligência Artificial capazes de apoiar auditorias, sumarizações, análises técnicas e validação automatizada de evidências.

Além disso, a Arquitetura atual não suporta os requisitos de integração financeira segura, processamento transacional com consistência ACID, conciliação em tempo real, split de pagamentos automatizado e governança de APIs exigidos pelo modelo operacional moderno das transações do órgão.

Diante desse cenário, torna-se imprescindível a contratação de solução tecnológica estruturante que permita a implementação e a operação de um ambiente moderno, escalável, seguro e orientado a serviços digitais de alta disponibilidade. A adoção de arquiteturas Cloud-Native, microsserviços, sincronização resiliente, inteligência artificial multimodal, mecanismos avançados de segurança e integração moderna é fundamental para garantir a continuidade do serviço público, a confiabilidade das informações, a proteção do cidadão, a eficiência administrativa e o atendimento às diretrizes de Governo Digital e de governança previstas na legislação vigente.

A contratação é, portanto, necessária para assegurar a transformação digital das atividades finalísticas do DETRAN-SP, garantir estabilidade operacional, promover a modernização dos serviços ao cidadão e fortalecer a capacidade institucional do órgão na gestão de processos críticos de trânsito, fiscalização, arrecadação e auditoria.

Plataforma de Pagamentos e Compensação (Detran Pay): a contratação atende a necessidade premente de resolver a fragmentação dos fluxos financeiros do DETRAN-SP, que atualmente gera riscos críticos de conciliação e dificuldades de auditoria. O sistema atuará como uma Clearing House interna, centralizando o split de pagamentos e garantindo a integração segura com o Banco do Brasil, o que é essencial para eliminar processos manuais, aumentar a transparência e modernizar a arrecadação do Estado.

Plataforma de Registro de Sinistros de Trânsito (RST): A contratação visa mitigar os gargalos críticos e as inconsistências geradas pela instabilidade de conectividade em campo na atual sistemática de registro de acidentes. A solução proposta é uma plataforma Cloud-Native, Offline-First que permitirá ao agente registrar o sinistro no local, mesmo sem internet, eliminando o retrabalho. Além disso, a integração com a Inteligência Artificial Generativa (Gemini Pro) é crucial para padronizar laudos e acelerar a liberação do documento ao cidadão de dias para horas.

Plataforma Estadual de Vistoria Veicular: A necessidade de substituição integral é impulsionada pela obsolescência tecnológica do sistema legado e-Vistoria e pela fragmentação dos dados de vistorias em múltiplas empresas, o que compromete a auditoria e a governança. A solução será uma plataforma unificada e escalável, construída em nuvem, cujo objetivo principal é ser o novo Backoffice de Vistoria, centralizando 100% dos laudos e estabelecendo uma Fonte Única da Verdade (SSOT) para modernizar a gestão e a fiscalização no Estado.

Plataforma Digital de Prova Prática (Exames de Habilitação): O sistema é fundamental para suprir a carência de evidências materiais auditáveis no processo de exame prático. A contratação visa prover Segurança Jurídica ao Estado por meio de uma arquitetura Offline-First que garante a resiliência operacional e a imutabilidade da prova. O uso de Georreferenciamento Avançado (Geofencing/Snap-to-Road) e de Auditoria Cognitiva (IA Gemini) garante a mitigação de fraudes geográficas e de conduta (coaçoão/suborno).

Reitera-se que a contratação é imprescindível para a transformação digital e segurança operacional do DETRAN-SP. A obsolescência tecnológica do ambiente legado representa risco à continuidade dos serviços públicos. A inovação tecnológica adotada em cada sistema visa garantir a estabilidade, a segurança, a rastreabilidade e a eficiência, elementos cruciais para o interesse público de um trânsito mais seguro e uma gestão transparente.

As razões concretas, a inovação tecnológica e o atendimento ao interesse público para cada sistema estruturante são detalhados a seguir:

a) Plataforma de Pagamentos e Compensação (DETRAN Pay):

- Fragmentação e Risco de Conciliação: A gestão financeira é fragmentada, exigindo processos manuais de conciliação (gargalo operacional), o que resulta em riscos críticos de inconsistência e dificuldades de auditoria financeira;
- Clearing House e Split de Pagamentos Centralizado (Cloud-Native): Centralização dos fluxos financeiros e transacionais, com garantia de consistência ACID (Atomicidade, Consistência, Isolamento e Durabilidade) e integração segura via APIs para split de pagamentos automatizado e conciliação em tempo real com o Banco do Brasil e demais agentes;
- Transparência, Arrecadação e Governança: Garante a fidedignidade e rastreabilidade dos fluxos financeiros do Estado, modernizando a arrecadação, eliminando fraudes por conciliação e assegurando a integridade dos recursos públicos destinados à segurança viária e à gestão administrativa.

b) Plataforma de Registro de Sinistros de Trânsito (RST)

- Inconsistência de Dados e Retrabalho: A dependência de conectividade constante na atual sistemática de registro de acidentes em campo leva a instabilidade, inconsistências, perda de dados e demora na liberação dos laudos ao cidadão (dias);
- Arquitetura Offline-First e Inteligência Artificial Generativa: Solução que permite a operação segura e completa sem internet, com sincronização resiliente. Uso de IA para padronização automática de laudos e sumários, acelerando a análise técnica e a liberação do documento de dias para horas;
- Celeridade, Segurança Viária e Atendimento ao Cidadão: Reduz a burocracia, melhora o tempo de resposta do Estado em situações de trânsito e aumenta a precisão dos laudos, fornecendo dados mais robustos para a análise de acidentalidade e políticas públicas de segurança viária.

c) Plataforma Digital de Prova Prática (Exames de Habilitação)

- Ausência de Evidências Materiais Auditáveis: O processo atual carece de mecanismos robustos para mitigar fraudes de conduta e geográficas (coaçoão, suborno) e não oferece evidências digitais imutáveis, gerando risco de insegurança jurídica para o Estado;
- Offline-First, Georreferenciamento Avançado e Inteligência Artificial (Auditoria Cognitiva): Arquitetura que garante a imutabilidade da prova e a resiliência operacional. Uso de Geofencing/Snap-to-Road para validação geográfica precisa e de IA (Auditoria Cognitiva) para detecção automatizada de condutas irregulares e apoio à decisão do examinador;
- Combate à Corrupção e Probidade Administrativa: Oferece segurança jurídica ao Estado por meio de uma cadeia de custódia digital completa, mitigando fraudes, coaçoão e suborno. Aumenta a confiabilidade do processo de habilitação, protegendo o interesse público de que apenas condutores aptos obtenham a CNH.

d) Plataforma Estadual de Vistoria Veicular

- Obsolescência e Fragmentação de Dados: O sistema legado (e-Vistoria) é obsoleto e os laudos estão fragmentados em bases de múltiplas empresas credenciadas, o que impede a auditoria centralizada e a governança efetiva sobre o processo de vistoria;

- **Backoffice Unificado em Nuvem (SSOT - Single Source of Truth):** Desenvolvimento de uma plataforma Cloud-Native, escalável e unificada, para centralizar a recepção, validação, auditoria e custódia de 100% dos laudos de vistoria no Estado, criando uma Fonte Única da Verdade da situação veicular;
- **Fiscalização, Combate à Fraude e Segurança Jurídica:** Fortalece a capacidade de fiscalização do DETRAN-SP, coibindo fraudes veiculares por meio da governança centralizada de dados, e assegura que a situação cadastral do veículo (componente essencial da segurança viária) seja baseada em informações íntegras e auditáveis.

3. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia da Informação	Bruno Zaia Boneto

4. Necessidades de Negócio

O DETRAN-SP identificou a necessidade de modernizar, desenvolver e evoluir seus sistemas finalísticos críticos em um ambiente tecnológico capaz de garantir alta performance, disponibilidade contínua, segurança avançada e aderência às diretrizes de transformação digital do Estado. A atual infraestrutura, fortemente baseada em soluções legadas e arquitetura on-premises, encontra-se limitada em escalabilidade, resiliência e capacidade de suporte às demandas crescentes da operação, impactando diretamente a continuidade do serviço público e a experiência do cidadão.

As necessidades do negócio convergem para a implementação integrada e modernizada de quatro soluções essenciais — Sistema de Prova Prática, Registro de Sinistro de Trânsito (RST), Plataforma Estadual de Vistoria (PEV) e Plataforma de Pagamentos (Detran Pay) — cuja operação é vital para a habilitação de condutores, gestão de sinistros, fiscalização de vistorias e processamento financeiro de receitas do órgão. Esses sistemas formam a espinha dorsal da atuação do DETRAN-SP, exigindo um ambiente tecnológico robusto, seguro e orientado a dados.

4.1. Continuidade Operacional em Campo (Offline-First)

As atividades finalísticas do DETRAN-SP são executadas majoritariamente em campo, em ambientes sujeitos a instabilidade ou ausência total de conectividade. A operação atual, dependente de conexão ativa e de sistemas centralizados, gera retrabalho, perda de evidências, inconsistências e atrasos que comprometem a efetividade da fiscalização e a credibilidade institucional.

Assim, o negócio requer soluções que adotem arquitetura Offline-First, permitindo:

- coleta e registro de faltas, biometria, áudios, fotos e geolocalização mesmo sem internet;
- sincronização automática, segura e transacional dos dados quando a conectividade retornar;
- continuidade operacional ininterrupta, eliminando paralisações e garantindo integridade das evidências.

Esse requisito é indispensável para a Prova Prática e para o RST, cuja operação ocorre frequentemente em zonas de sombra de sinal e demanda resposta imediata, precisa e auditável.

4.2. Segurança Jurídica, Auditoria e Integridade de Evidências

O DETRAN-SP necessita de soluções que reforcem a confiabilidade das informações e a segurança jurídica dos atos administrativos, mitigando riscos de contestações, fraudes e inconsistências. Para isso, os novos sistemas devem incorporar:

- Inteligência Artificial Generativa para transcrição de áudios, análise cognitiva, sumarização de depoimentos e geração de narrativas estruturadas;
- Geolocalização avançada com geofencing e auditoria de trajeto (Snap-to-Road), garantindo que provas e registros ocorram em locais autorizados;
- cadeia de custódia digital, assegurando imutabilidade de evidências como fotos, vídeos, áudios e registros de GPS;
- trilhas de auditoria completas, com logs imutáveis e auditáveis em todas as operações.

Essas funcionalidades são determinantes para:

- evitar fraudes na Prova Prática;
- garantir precisão na classificação de danos no RST;
- preservar a integridade de laudos periciais;
- assegurar conformidade regulatória nos processos administrativos.

4.3. Modernização Financeira e Operação de Clearing House

O fluxo financeiro do DETRAN-SP é estratégico e exige alto nível de segurança, rastreabilidade e confiabilidade. A evolução da plataforma de pagamentos (Detran Pay) deve contemplar:

- criação de um Core Bancário capaz de operar como uma Clearing House interna, centralizando o split de pagamentos entre órgão e credenciados;
- conciliação financeira em tempo real;
- integração segura com instituições financeiras, seguindo padrões de Open Finance;
- monitoramento contínuo de ameaças e blindagem cibernética avançada;
- consistência ACID para todas as transações.

Esses requisitos respondem à necessidade do negócio de eliminar divergências financeiras, reduzir riscos operacionais e garantir aderência às normas fiscais e de controle.

4.4. Consolidação de Dados e Fonte Única da Verdade (SSOT)

O DETRAN-SP necessita substituir sistemas fragmentados, heterogêneos e tecnicamente defasados por plataformas unificadas, que permitam governança centralizada e análise em grande escala.

A Plataforma Estadual de Vistoria e os demais sistemas críticos devem operar sobre:

- um repositório central unificado (Data Warehouse / Data Lake);
- padronização de laudos e evidências;
- integração simplificada via APIs modernas;
- capacidade analítica para auditorias, inteligência de fiscalização e tomada de decisão.

A centralização dos dados de vistoria, sinistros, provas e pagamentos permitirá aumentar a transparência, reduzir fraudes, aprimorar o controle interno e melhorar a qualidade das informações disponibilizadas ao cidadão e aos órgãos de controle.

4.5. Superação das Limitações da Infraestrutura Atual

A infraestrutura existente não dispõe de:

- elasticidade para absorver picos de demanda;
- ambiente adequado para execução de microsserviços em escala;
- criação rápida de ambientes paralelos para desenvolvimento, testes e homologação;
- recursos nativos para IA, mensageria, sincronização resiliente ou geolocalização de alta precisão;
- mecanismos adequados de segurança de borda, criptografia avançada e monitoramento de ameaças;
- governança moderna de APIs, essencial para integrações críticas.

Essas limitações impedem a execução eficiente das atividades do DETRAN-SP e restringem a adoção de práticas modernas de desenvolvimento, DevSecOps, SRE e engenharia de dados.

Diante das demandas operacionais, tecnológicas e regulatórias identificadas, a contratação de serviços especializados de desenvolvimento, modernização e sustentação de sistemas é imprescindível para que o DETRAN-SP disponha de um ambiente tecnológico resiliente, moderno, escalável e seguro. A evolução dos quatro sistemas críticos permitirá garantir a continuidade dos serviços públicos essenciais, fortalecer a governança institucional, ampliar a segurança jurídica, promover transparência e assegurar aderência às diretrizes de transformação digital do Estado.

5. Necessidades Tecnológicas

A definição das necessidades tecnológicas decorre da análise integrada dos sistemas finalísticos e corporativos que compõem o ecossistema digital do DETRAN-SP. Impõe-se o mapeamento de um conjunto de necessidades tecnológicas mínimas que devem orientar o desenvolvimento e a modelagem dos sistemas no ambiente de nuvem do DETRAN-SP.

Essas necessidades traduzem, em linguagem técnica, as capacidades essenciais que o ambiente de nuvem gerenciado deverá possuir para viabilizar a implantação e a operação dos novos sistemas estratégicos.

5.1. Necessidade de Infraestrutura Computacional Escalável (Aderência ao Software)

O ambiente deve suportar escalabilidade vertical e horizontal, permitindo a ampliação ou redução de recursos conforme a demanda real dos serviços. Tal característica é indispensável para assegurar:

- Suporte ao Desenvolvimento e CI/CD: Ambientes segregados e ajustáveis (Desenvolvimento, Homologação, Produção e Contingência) são essenciais para o Ciclo de Vida de Software Ágil (DevOps).
- Cargas Intensivas: Capacidade computacional suficiente para cargas intensivas que dependem de processamento geoespacial (PEV, Prova Prática), algoritmos de validação biométrica e análise multimídia/IA/ML (RST, Prova Prática).
- Escalabilidade para Microsserviços: A solução deve ser baseada em microsserviços e contêineres (Serverless/Cloud Run) para garantir escalabilidade automática durante picos (ex: feriados em RST), além de suportar funções serverless de alta intensidade.

5.2. Necessidade de Armazenamento Massivo, Durável e Economicamente Gerenciável

O ambiente deve gerir um volume crescente de informações, especialmente dos novos sistemas desenvolvidos, garantindo:

- Volumetria Crescente e Diversificada: Suporte a milhões de arquivos por mês, incluindo imagens e vídeos de Vistorias (PEV), evidências de rotas e auditorias de Provas Práticas e laudos/registros de Sinistros de Trânsito (RST).
- Processamento Analítico: O armazenamento deve ser compatível com ferramentas de Big Data e IA/ML, com Data Warehouse (BigQuery) populado, fundamental para painéis gerenciais (Looker) e o Data Lake Financeiro (Detran Pay).
- Durabilidade e Auditabilidade: Garantia de durabilidade e integridade para provas jurídicas e evidências digitais, com logs de acesso e modificação imutáveis (Cloud Logging) para a cadeia de custódia do RST.

5.3. Necessidade de Alta Disponibilidade, Redundância e Continuidade Operacional

A infraestrutura deve assegurar alta disponibilidade para todos os sistemas críticos, com arquiteturas resilientes entre múltiplas regiões e múltiplos provedores.

- Resiliência Offline-First: Mecanismos que garantam sucesso de sincronização de 100%, impedindo que dados coletados offline sejam perdidos ao reconectar (Requisito crítico do RST e Prova Prática).
- Resiliência Assíncrona: Utilização de filas de mensageria (Pub/Sub) para garantir o processamento assíncrono e resiliente das evidências (fotos /vídeos), essencial para RST.
- DR e Failover: Ambientes de Recuperação de Desastres (DR) estruturados e a capacidade de alternância rápida entre ambientes primários e secundários, essenciais para os sistemas transacionais (Detran Pay) e de captura em campo.

5.4. Necessidade de Segurança da Informação, Proteção de Dados e Governança de Identidades

A segurança deve ser tratada como componente transversal, com mecanismos consistentes entre os provedores (Governança Unificada), garantindo:

- Criptografia para Operações em Campo: Criptografia em Repouso no Dispositivo (ex: SQLCipher) para o banco de dados local do tablet, crucial para o Sistema de Prova Prática e RST.
- Blindagem Financeira e AppSec: A aplicação móvel e o Detran Pay devem passar por testes rigorosos de segurança estática (SAST) e dinâmica (DAST) para prevenir vulnerabilidades financeiras.
- Proteção de Borda: Implementação de WAF (Web Application Firewall) com regras de geobloqueio para impedir acesso administrativo fora do Brasil.
- Governança LGPD: A solução deve garantir o mascaramento de dados sensíveis nos ambientes de testes e homologação.

5.5. Necessidade de Interoperabilidade, Integração e Baixa Latência

A futura solução deverá suportar comunicação segura e de baixa latência entre os novos sistemas e o legado:

- Integração Governamental: Suporte à integração gov.br para autenticação segura (Prova Prática, RST, Detran Pay).
- Gateway de APIs: Oferecer API Management para padronizar e proteger a comunicação com sistemas externos, como o Banco do Brasil (Detran Pay).
- Integração com Legado: Prever API de Integração com Legado para envio de resultados.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

A escolha da solução de Tecnologia da Informação mais adequada às demandas institucionais do DETRAN-SP deve observar um conjunto articulado de requisitos técnicos, operacionais, jurídicos e estratégicos que garantam que a decisão futura seja plenamente fundamentada, sustentável e alinhada aos objetivos de modernização do órgão. Tais requisitos visam assegurar que qualquer alternativa tecnológica considerada pela Administração possua capacidade real, comprovável e duradoura para atender às necessidades mapeadas no presente Estudo Técnico Preliminar, sem criar dependência excessiva, sem comprometer a evolução das políticas públicas de trânsito e sem limitar a expansão futura dos serviços digitais.

Importante destacar que esses requisitos não configuram a seleção prévia de fornecedor, plataforma ou arquitetura. Representam, sim, o conjunto mínimo e indispensável de condições que devem orientar a Administração na formulação do Termo de Referência, na comparação das alternativas disponíveis no mercado e na decisão final pela solução de TIC a ser contratada.

A observância desses requisitos é condição necessária para que a contratação assegure continuidade de serviços, governança, eficiência operacional, segurança da informação, escalabilidade, economicidade e aderência às diretrizes de governo digital.

6.1. Aderência às diretrizes de transformação digital, governança de TIC e políticas institucionais

A solução tecnológica a ser considerada deverá apresentar aderência plena ao conjunto de políticas, diretrizes e instrumentos de planejamento que orientam a transformação digital no âmbito do Governo do Estado de São Paulo e do DETRAN-SP. Essa aderência é condição essencial para garantir que o investimento público seja realizado de forma estratégica, sustentável e alinhada à evolução institucional esperada para os próximos ciclos de modernização.

A alternativa a ser selecionada deverá, obrigatoriamente:

- Atender às diretrizes estaduais de digitalização do serviço público, interoperabilidade, integração sistêmica e prestação digital ampliada, assegurando que os novos sistemas possam dialogar entre si, compartilhar dados de forma segura e evitar ilhas tecnológicas que comprometam a escala e o valor público gerado.
- Estar alinhada às estratégias estaduais de governança de dados, proteção da informação, cibersegurança e anonimização, respeitando padrões técnicos e normativos aplicáveis à Administração Pública, com especial atenção aos requisitos de integridade, confidencialidade, disponibilidade e rastreabilidade de dados sensíveis.
- Ser compatível com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) ou documento equivalente do DETRAN-SP, garantindo coerência com a visão institucional de evolução arquitetural, sustentabilidade tecnológica, maturidade digital e integração com sistemas corporativos e finalísticos do órgão.
- Adotar boas práticas reconhecidas de governança de TIC, incluindo princípios de priorização de serviços digitais, simplificação administrativa, automação inteligente de processos, uso racional e otimizado de recursos computacionais e adoção de tecnologias escaláveis, resilientes e interoperáveis.
- Estar alinhada ao modelo de Administração Pública Digital, garantindo convergência com:
 - políticas estaduais de governo digital;
 - padrões de identidade digital e autenticação cidadã;
 - estratégias de gestão orientada a dados;
 - requisitos de monitoramento contínuo, prestação de contas e transparência.

Racionalidade do Requisito

Esse requisito tem por finalidade assegurar que a solução tecnológica escolhida:

- evite fragmentação entre sistemas e repositórios de dados;
- reduza retrabalho futuro decorrente de escolhas tecnológicas incompatíveis com a evolução arquitetural prevista;
- garanta sinergia com iniciativas de transformação digital desenvolvidas no âmbito do Governo do Estado;
- maximize a reutilização de ativos, boas práticas, integrações e padrões adotados institucionalmente;
- preserve a coerência estratégica entre a contratação, o ciclo de vida da solução e os objetivos de modernização do DETRAN-SP.

Dessa forma, assegura-se que a solução final não seja apenas tecnicamente adequada, mas também estrategicamente sustentável, institucionalmente coerente e juridicamente alinhada aos instrumentos de governança vigentes.

6.2. Conformidade normativa e aderência à legislação aplicável às contratações de TIC

A solução tecnológica a ser selecionada deverá observar rigorosamente o arcabouço normativo que rege as contratações públicas de Tecnologia da Informação e Comunicação, assegurando que toda a modelagem, comparação de alternativas, especificação e futura contratação sejam plenamente compatíveis com as exigências legais, regulatórias e procedimentais aplicáveis ao DETRAN-SP.

Para tanto, a alternativa analisada deverá comprovar aderência integral:

- À Lei nº 14.133/2021, particularmente quanto:
- ao dever de planejamento prévio (arts. 6º e 18);
- à motivação e fundamentação técnica das decisões administrativas;
- à gestão de riscos, transparência e governança das contratações;
- à economicidade e à vantagem técnica e operacional;
- à segregação de fases, critérios objetivos de seleção e avaliação de propostas;
- à necessidade de garantir continuidade do serviço público e mitigação de dependência tecnológica.
- Aos normativos estaduais aplicáveis à TIC, incluindo diretrizes de:
- arquitetura corporativa;
- padronização de serviços;
- contratação e gestão de soluções em nuvem;
- segurança da informação e proteção de dados;
- boas práticas de desenvolvimento seguro, interoperabilidade e modernização tecnológica.
- À legislação e diretrizes relacionadas à proteção de dados pessoais e à classificação das informações, assegurando cumprimento de:
- regras de tratamento, compartilhamento e anonimização de dados pessoais e sensíveis;
- mecanismos de controle de acesso, segregação de ambientes e trilhas de auditoria;
- requisitos de confidencialidade, integridade e disponibilidade relacionados a operações críticas (habilitação, vistoria, sinistros e pagamentos).
- Às orientações dos órgãos de controle interno e externo sobre contratações de TIC, incorporando:
- boas práticas recomendadas para mitigação de riscos contratuais;
- critérios de avaliação de soluções de software, infraestrutura e nuvem;
- padrões de governança, segregação de tarefas, planejamento de capacidade e continuidade.
- Aos requisitos mínimos para soluções em ambiente de nuvem definidos por órgãos centrais de TI e instâncias regulatórias, assegurando conformidade com padrões de:
- segurança cibernética;
- proteção de cargas críticas;
- gestão de identidade, criptografia e redundância;
- operacionalização de ambientes multi-região, sincronização resiliente e mecanismos de Disaster Recovery.
- Às restrições legais referentes a dados pessoais, dados sensíveis, evidências digitais e informações sujeitas a sigilo administrativo ou legal, garantindo que o desenho da solução respeite os limites normativos aplicáveis aos serviços finalísticos do DETRAN-SP (habilitação, trânsito, fiscalização e arrecadação).

Finalidade do Requisito

O atendimento integral a esse conjunto de critérios:

- assegura que a solução tecnológica selecionada seja juridicamente sustentável,

- reforça a aderência aos princípios da Administração Pública,
- garante conformidade regulatória ao longo de todo o ciclo de vida da solução,
- evita riscos de litígios, responsabilizações ou fragilidades contratuais,
- e contribui para a segurança, transparência e integridade das atividades finalísticas do DETRAN-SP.

6.3. Aderência à arquitetura tecnológica atual e ao planejamento evolutivo

A solução tecnológica a ser considerada deverá apresentar plena compatibilidade com a arquitetura vigente do DETRAN-SP e, simultaneamente, capacidade de acompanhar a evolução planejada para o ecossistema digital do órgão. A aderência à arquitetura atual e futura é fundamental para evitar rupturas desnecessárias, maximizar o reaproveitamento de componentes já consolidados e assegurar que a modernização dos sistemas finalísticos ocorra de forma ordenada, segura e sustentável.

Para isso, a alternativa tecnológica deverá:

- Integrar-se de forma natural, segura e progressiva ao ecossistema de sistemas finalísticos e corporativos do DETRAN-SP, permitindo interconexão fluida com módulos legados, portais corporativos, bases administrativas, soluções de arrecadação, motor de pagamentos e sistemas regulatórios que compõem a estrutura operacional existente.
- Garantir continuidade operacional dos ambientes atuais, evitando interrupções prolongadas, reescritas desnecessárias ou substituições abruptas de componentes críticos. A solução deve ser capaz de coexistir com o ambiente vigente durante fases de migração, estabilização ou transição assistida, permitindo um processo evolutivo gradativo.
- Suportar introdução futura de tecnologias emergentes, incluindo:
 - modelos avançados de inteligência artificial e aprendizado de máquina;
 - análises preditivas e cognitivas;
 - processamento multimodal e geoespacial de alta complexidade;
 - capacidades de auditoria avançada baseadas em dados;
 - automação de processos e monitoramento inteligente.
 Essa flexibilidade é essencial para assegurar longevidade da solução e capacidade de absorver inovações tecnológicas ao longo do ciclo de vida dos sistemas.
- Manter alinhamento com padrões institucionais de desenvolvimento, integração, dados e segurança, incluindo convenções técnicas já utilizadas pelo órgão, padronização de APIs, práticas modernas de DevSecOps, estruturas de dados amplamente adotadas e requisitos de segurança e privacidade consolidados. A solução deve complementar, e não substituir, boas práticas já institucionalizadas.
- Ser compatível com cenários de operação simultânea em múltiplas plataformas tecnológicas, inclusive ambientes multicloud e híbridos, permitindo que a evolução para novos provedores, tecnologias ou arquiteturas ocorra sem dependência excessiva ou limitação técnica. Essa compatibilidade reduz riscos de lock-in, aumenta a flexibilidade estratégica e promove autonomia para a Administração.

Finalidade Estratégica do Requisito

Esse requisito assegura que a escolha tecnológica:

- minimize riscos de desalinhamento entre sistemas novos e legados;
- otimize o reaproveitamento de investimentos já realizados em infraestrutura, desenvolvimento e capacitação;
- viabilize transições técnicas suaves, sem impacto sobre serviços críticos ou sobre o cidadão;
- permita evolução arquitetural contínua, organizada e sustentável;
- garanta compatibilidade com a visão de longo prazo prevista no planejamento tecnológico do DETRAN-SP.

Ao observar tais condições, a Administração garante que a solução tecnológica a ser contratada não apenas resolva necessidades imediatas, mas também sirva como base sólida para a transformação digital contínua da instituição.

6.4. Capacidade de integração, interoperabilidade e conectividade segura

A solução tecnológica a ser futuramente especificada deverá garantir capacidade plena de integração, interoperabilidade e comunicação segura entre todos os sistemas que compõem o ecossistema digital do DETRAN-SP, bem como com bases externas, dispositivos móveis e sistemas de outros entes públicos. Para isso, deverá adotar padrões modernos de integração, arquiteturas orientadas a serviços e mecanismos consolidados de segurança e proteção de dados.

A alternativa considerada deverá obrigatoriamente ser capaz de:

- Oferecer mecanismos padronizados de integração com sistemas internos e externos, utilizando práticas modernas de API Management, padrões RESTful, mensageria assíncrona e autenticação federada, permitindo interoperabilidade com bases corporativas do DETRAN-SP, sistemas de arrecadação, motor financeiro, plataformas de vistoria, soluções de habilitação e demais sistemas finalísticos.
- Viabilizar comunicação segura entre ambientes heterogêneos, inclusive aplicações legadas on-premises, microsserviços em nuvem, sistemas móveis em campo (tablets e smartphones) e serviços governamentais federais e estaduais. Deve ainda garantir criptografia ponta a ponta e segregação de fluxos sensíveis.
- Assegurar interoperabilidade com bases federais e estaduais estratégicas, como sistemas de identificação civil, validação biométrica, serviços de autenticação, cadastros regulatórios e bases necessárias às atividades de trânsito. A solução deverá garantir conformidade com protocolos oficiais de integração exigidos pelas esferas federal e estadual.
- Suportar altos volumes de tráfego e operações de baixa latência, garantindo estabilidade, resiliência e desempenho compatíveis com demandas críticas — como envio massivo de evidências de sinistros, auditoria de vistorias, sincronização de provas práticas, conciliação financeira do Detran Pay e fluxos de autenticação simultânea de milhares de usuários.
- Operar com arquitetura favorável à expansão horizontal e vertical de integrações, permitindo que novos módulos, serviços, bases de dados ou parceiros institucionais sejam incorporados de forma simples, escalável e segura, sem necessidade de retrabalhos extensos ou reconstruções sistêmicas.

Finalidade do Requisito

A interoperabilidade é componente central da estratégia digital do DETRAN-SP e representa condição indispensável para:

- assegurar a continuidade dos serviços prestados ao cidadão, sem interrupções causadas por incompatibilidade tecnológica;
- evitar a formação de ilhas tecnológicas isoladas, que dificultam compartilhamento de dados, elevam custos e reduzem a eficiência;
- permitir evolução e integração contínua de novos módulos ou sistemas finalísticos;
- garantir uniformidade de padrões, integridade das informações e comunicação confiável entre todas as camadas tecnológicas;
- viabilizar que o ecossistema do DETRAN-SP opere de forma altamente conectada, segura e orientada a dados.

Esse requisito, portanto, consolida a necessidade de que a solução a ser contratada possua capacidade robusta, flexível e sustentável de integração, assegurando alinhamento arquitetural com o presente e com o futuro digital da instituição.

6.5. Aderência a requisitos reforçados de segurança da informação e proteção de dados

Dada a elevada criticidade das atividades desempenhadas pelo DETRAN-SP — que envolvem operações de fiscalização, gestão de sinistros, habilitação de condutores, vistoria veicular, processamento financeiro e tratamento contínuo de dados pessoais e sensíveis — a solução tecnológica a ser selecionada deverá obedecer rigorosamente aos requisitos reforçados de segurança da informação, proteção de dados e governança institucional. Esses requisitos visam garantir absoluta integridade, confidencialidade, disponibilidade e autenticidade das informações processadas.

Para isso, a solução deverá, no mínimo:

- Implementar mecanismos robustos e escaláveis de controle de acesso e autenticação, baseados em identidade, com aplicação de princípios de privilégio mínimo, autenticação multifator, segregação por perfis funcionais e níveis diferenciados de acesso conforme a criticidade dos serviços utilizados.
A solução deve ainda permitir integração com mecanismos modernos de identidade digital governamental e gestão centralizada de credenciais.
- Proteger dados em trânsito e em repouso com criptografia avançada, assegurando sigilo, integridade e resistência à adulteração, tanto no armazenamento em nuvem quanto em dispositivos móveis utilizados em campo.
Isso inclui, obrigatoriamente:
 - criptografia local no dispositivo (ex.: bases offline da Prova Prática e RST),
 - criptografia ponta a ponta entre aplicativos móveis e APIs,
 - mecanismos para evitar extração, cópia ou interceptação indevida de evidências.

- Assegurar segregação rigorosa de ambientes, funções, perfis e cargas de trabalho, conforme melhores práticas de segurança, permitindo isolamento entre ambientes de desenvolvimento, testes, homologação e produção, prevenindo contaminações cruzadas, acesso indevido a dados sensíveis e exposição inadvertida de informações de operação.
- Dispor de mecanismos de prevenção, detecção e resposta a incidentes, com monitoramento contínuo (24x7), identificação de comportamentos anômalos, bloqueio automatizado de acessos suspeitos e capacidade de resposta imediata a tentativas de ataque, fraude ou manipulação. A solução deverá contemplar:
 - detecção de intrusão;
 - análise de padrões irregulares em transações financeiras (Detran Pay);
 - monitoramento de alterações suspeitas em laudos, sinistros, provas e dados de vistoria;
 - registro e tratamento estruturado de incidentes.
- Manter trilhas de auditoria completas e imutáveis, assegurando rastreabilidade integral das operações críticas, incluindo:
 - alterações em cadastros, laudos, vistoria, sinistros e evidências de prova;
 - modificações em parâmetros de sistema;
 - operações financeiras;
 - consultas e acessos a informações sensíveis.
 Todas as ações relevantes devem ser registradas com data, hora, usuário, origem, ação e resultado.
- Garantir conformidade com a legislação vigente de proteção de dados pessoais, em especial a Lei Geral de Proteção de Dados (LGPD), além das políticas institucionais correlatas e dos normativos estaduais aplicáveis a tratamento, armazenamento, anonimização, compartilhamento e eliminação de dados.
- Assegurar a integridade, autenticidade e confiabilidade de evidências digitais, tais como:
 - registros de vistorias com georreferenciamento,
 - arquivos multimídia de sinistros e provas práticas,
 - fotos, vídeos e trilhas de movimentação,
 - croquis geoespaciais,
 - evidências de dispositivos móveis usados em campo,
 - logs e registros financeiros do Detran Pay.
 A solução deve incorporar mecanismos que impeçam adulteração, substituição ou supressão dessas evidências.

Finalidade Estratégica do Requisito

A observância rigorosa deste conjunto de requisitos fortalece a capacidade institucional do DETRAN-SP em:

- preservar a confiabilidade dos dados e assegurar a validade jurídica das operações;
- mitigar riscos relacionados a fraudes, adulterações, vazamentos ou perda de informações;
- proteger o cidadão e a Administração contra vulnerabilidades tecnológicas;
- atender rigorosamente às exigências legais de proteção de dados e segurança;
- sustentar a continuidade dos serviços críticos mesmo diante de tentativas de ataque ou instabilidade operacional;
- permitir auditoria integral dos processos, reforçando transparência e governança institucional.

Trata-se, portanto, de um requisito essencial para garantir que a solução tecnológica a ser contratada opere em conformidade com os mais elevados padrões de segurança e proteção de dados aplicáveis ao setor público.

6.6. Governança financeira, previsibilidade de custos e aderência a práticas de gestão de gastos em TIC

A solução tecnológica a ser futuramente selecionada deve possibilitar uma governança financeira sólida, transparente e alinhada às melhores práticas de gestão de custos em TIC, assegurando que o DETRAN-SP tenha pleno controle sobre o consumo de recursos, previsibilidade orçamentária e capacidade de ajustar os gastos de acordo com a dinâmica operacional dos serviços públicos de trânsito. Considerando o caráter crítico, contínuo e de alta volumetria dos sistemas institucionais, torna-se indispensável que a solução permita administração eficiente e racional dos custos ao longo de todo o ciclo de vida da contratação.

Assim, a solução deverá:

- Fornecer visibilidade granular, precisa e auditável do consumo de recursos tecnológicos, permitindo ao DETRAN-SP acompanhar, em tempo real, a utilização de processamento, armazenamento, tráfego, serviços de dados, integrações, workloads de IA e consumo de APIs, inclusive com segregação por sistema, por unidade de negócio e por ambiente.
- Permitir ajustes finos, contínuos e dinâmicos para otimização de custos, suportando mecanismos automáticos e manuais de ajuste de capacidade, autoscaling controlado, otimização de performance, desligamento de serviços ociosos e adequação de cargas a horários de menor custo operacional.
- Favorecer previsibilidade orçamentária e estabilidade financeira, reduzindo a volatilidade no faturamento e permitindo ao DETRAN-SP estimar com maior precisão os custos mensais e anuais dos serviços, mitigando o risco de oscilações inesperadas decorrentes de mudanças de demanda, picos sazonais ou acréscimos não planejados.
- Possibilitar alocação eficiente e estratégica de cargas entre ambientes, observando critérios de custo-benefício que considerem a criticidade, disponibilidade necessária, desempenho, compliance e impacto ao cidadão, garantindo que ambientes críticos recebam capacidade prioritária enquanto ambientes menos sensíveis operem com custos otimizados.
- Apoiar a identificação e correção de desperdícios, incluindo:
 - detecção de recursos superdimensionados,
 - identificação de serviços ociosos ou subutilizados,
 - alertas automáticos sobre anomalias de consumo,
 - relatórios que permitam ações corretivas para contenção de gastos.
Essa capacidade contribui para mitigar riscos de sobrecarga financeira ao longo do contrato.
- Permitir adequação automática e planejada da capacidade de infraestrutura aos ciclos operacionais e sazonalidades institucionais, considerando períodos de maior demanda, tais como:
 - picos de vistorias veiculares (PEV);
 - temporadas de maior volume de sinistros (RST);
 - intensificação de provas práticas em determinadas regiões ou épocas do ano;
 - sazonalidade do processamento financeiro no Detran Pay;
 - crescimento temporário de acessos por demandas do cidadão.
A solução deve acompanhar esses ciclos sem gerar sobrecusto desnecessário.

Finalidade Estratégica do Requisito

A observância desse conjunto de critérios visa assegurar que a contratação:

- seja financeiramente sustentável ao longo do tempo;
- reduza riscos de descontrole orçamentário, especialmente em ambientes de alta elasticidade;
- garanta controle institucional sobre gastos, evitando dependência ou opacidade na cobrança de serviços;
- contribua para a eficiência na utilização dos recursos públicos;
- alinhe-se às práticas modernas de FinOps, permitindo gestão ativa, previsível e otimizada dos custos em nuvem;
- atenda, simultaneamente, às necessidades críticas do DETRAN-SP e às limitações inerentes ao orçamento público.

Trata-se, portanto, de requisito indispensável para garantir maturidade financeira, transparência, sustentabilidade e segurança na adoção de soluções tecnológicas estratégicas.

6.7. Atendimento a requisitos de disponibilidade, continuidade e recuperação de desastres

A solução tecnológica a ser selecionada deverá demonstrar capacidade plena de atender a requisitos rigorosos de disponibilidade, continuidade operacional e recuperação de desastres, compatíveis com a natureza essencial dos serviços prestados pelo DETRAN-SP e com o impacto direto que eventuais indisponibilidades podem gerar para o cidadão, credenciados, agentes públicos e para a própria execução das políticas de trânsito.

Dada a criticidade dos sistemas finalísticos — vistorias veiculares, registro de sinistros, provas práticas, arrecadação e fluxos financeiros — a solução deverá contemplar, obrigatoriamente:

- Níveis de disponibilidade compatíveis com serviços essenciais, garantindo que o funcionamento dos sistemas seja contínuo, seguro e estável. Os níveis específicos de SLA e SLO serão definidos em etapa posterior do planejamento, mas deverão refletir padrões elevados de operação, sem degradações significativas em horários de pico, feriados, operações especiais ou eventos climáticos adversos.
- Arquitetura resiliente, distribuída e livre de pontos únicos de falha, incluindo:
 - balanceamento de carga,
 - replicação geográfica,
 - segmentação de serviços,
 - mecanismos de isolamento de falhas,
 - infraestrutura redundante em ambientes distintos (regiões, zonas ou provedores).
Essa resiliência deve garantir que falhas localizadas não provoquem interrupção integral dos sistemas críticos.
- Recursos de tolerância a falhas e mecanismos de recuperação automática ou assistida, capazes de detectar degradações, reiniciar serviços comprometidos, reencaminhar fluxos de processamento e restabelecer estados operacionais de forma autônoma ou supervisionada. Tais mecanismos são indispensáveis para garantir continuidade de operações como:
 - fluxo de sinistros em processamento,
 - migração de laudos de vistoria,
 - sincronização de dados offline das provas práticas,
 - conciliação financeira em execução.
- Estratégias estruturadas de Recuperação de Desastres (Disaster Recovery – DR), que contemplem:
 - ambientes secundários preparados para assumir a operação de maneira rápida e eficiente;
 - objetivos de tempo de recuperação (RTO) e de ponto de recuperação (RPO) compatíveis com a essencialidade das operações do DETRAN-SP;
 - procedimentos de failover e fallback documentados, testados e auditáveis;
 - mecanismos de versionamento, rastreabilidade e restauração de dados.
Essas estratégias devem cobrir tanto eventos tecnológicos quanto indisponibilidades decorrentes de fatores externos (climáticos, energéticos, incidentes físicos, falhas massivas de rede).
- Mecanismos eficazes de prevenção de indisponibilidades prolongadas, garantindo que falhas em infraestrutura, integrações externas, serviços móveis em campo ou fluxos financeiros não comprometam a prestação do serviço público. Esses mecanismos devem considerar:
 - operação offline com sincronização segura (Prova Prática e RST),
 - buffer temporário de evidências (fotos, vídeos, logs),
 - redundância de gateways de API,
 - contingência para operações financeiras do Detran Pay,
 - manutenção contínua de canais essenciais para cidadão e credenciados.

Finalidade Estratégica do Requisito

Esse requisito é mandatório para assegurar que a solução tecnológica:

- mantenha a prestação dos serviços de trânsito de forma contínua, ininterrupta e segura;
- minimize impactos ao cidadão e aos credenciados em situações de falha técnica;

- garanta proteção institucional frente a riscos operacionais e reputacionais;
- preserve a integridade das operações críticas, mesmo diante de falhas amplas;
- esteja sincronizada com o modelo de resiliência esperado de soluções estratégicas para o Estado.

A disponibilidade e a continuidade operacional são, portanto, pilares indispensáveis para o funcionamento adequado do ecossistema digital do DETRAN-SP e devem ser observadas com rigor em qualquer alternativa tecnológica considerada.

6.8. Governança de ambientes distribuídos e administração centralizada de múltiplas plataformas

A solução tecnológica a ser considerada deve ser capaz de operar e governar ambientes computacionais distribuídos, heterogêneos e potencialmente multicloud, assegurando que o DETRAN-SP disponha de mecanismos consolidados de gestão, controle, segurança e supervisão sobre todos os recursos tecnológicos utilizados. Em um cenário em que diferentes sistemas finalísticos podem demandar soluções distintas — ambientes móveis, serviços em nuvem, APIs externas, legado on-premises e plataformas transacionais — torna-se essencial dispor de uma camada de governança que unifique a administração desses componentes sem comprometer a autonomia institucional.

Assim, a alternativa tecnológica deverá permitir:

- Integração centralizada da gestão de identidades, acessos, políticas de segurança e auditorias, garantindo que mecanismos de autenticação, autorização, segregação de privilégios e trilhas de auditoria funcionem de modo uniforme, independentemente do ambiente em que cada componente esteja hospedado. Essa unificação deve abranger governança de APIs, logs, chaves, tokens, perfis funcionais e políticas de conformidade.
- Provisionamento e desprovisionamento coordenados de recursos, permitindo que novos serviços, ambientes e componentes possam ser criados, configurados e desativados de forma padronizada, reduzindo riscos de configuração divergente, falhas operacionais e exposição indevida de dados. Esse provisionamento deve seguir modelos automatizados, consistentes e auditáveis.
- Consolidação de visão financeira e operacional dos diferentes ambientes tecnológicos, permitindo monitoramento unificado de consumo, performance, custos, capacidade, incidentes, saúde dos serviços e indicadores críticos de disponibilidade. Essa visibilidade integrada é essencial para tomada de decisão em tempo hábil, otimização de recursos e gestão eficaz das operações.
- Operação simultânea em múltiplos provedores de nuvem ou plataformas tecnológicas, quando requerido, garantindo interoperabilidade, padronização, portabilidade e continuidade operacional. Isso inclui capacidade de orquestração de serviços em ambientes híbridos (legado + nuvem) e multicloud, com políticas centralizadas de segurança, identidade e conformidade.
- Autonomia da Administração para mover cargas de trabalho entre ambientes, respeitando critérios técnicos (desempenho, latência, segurança, disponibilidade) ou estratégicos (redução de custos, mitigação de riscos, otimização de performance). Tal autonomia reduz barreiras para ajustes evolutivos, reforça flexibilidade institucional e assegura soberania sobre os recursos tecnológicos.
- Redução dos riscos de dependência tecnológica excessiva (“lock-in”), conferindo ao DETRAN-SP capacidade de evoluir para novos ambientes, tecnologias ou arquiteturas sem necessidade de reescritas dispendiosas, atrasos operacionais ou interrupção dos serviços finalísticos. A solução deve facilitar migrações planejadas, interoperabilidade técnica e compatibilidade com padrões abertos.

Finalidade Estratégica do Requisito

A implementação dessa camada de governança integrada:

- evita fragmentação operacional entre nuvem, legado, dispositivos móveis e integrações externas;
- fortalece o controle institucional sobre identidades, dados, custos, riscos e fluxos críticos;
- garante coerência e padronização na operação de sistemas estratégicos e sensíveis;
- amplia a autonomia técnica do DETRAN-SP, reduzindo exposição a dependências tecnológicas;
- viabiliza evolução arquitetural compatível com as políticas de governo digital e boas práticas de gestão de TIC.

Trata-se de requisito essencial para que o DETRAN-SP governe de forma eficiente, segura e centralizada um ecossistema cada vez mais distribuído, complexo e orientado a múltiplas plataformas.

6.9. Requisitos de auditabilidade, rastreabilidade e transparência

A solução tecnológica a ser selecionada deverá assegurar níveis elevados de auditabilidade, rastreabilidade e transparência, compatíveis com a natureza sensível das informações processadas pelo DETRAN-SP e com as responsabilidades legais que recaem sobre os serviços de trânsito, fiscalização, arrecadação e gestão de identidades. Tais mecanismos são essenciais para garantir integridade de processos, proteção ao cidadão, segurança jurídica e conformidade com as exigências dos órgãos de controle interno e externo.

Nesse sentido, a solução deverá garantir, no mínimo:

- Registros detalhados, completos e imutáveis de acessos, eventos, integrações, transações e operações críticas, incluindo:
 - consultas e atualizações de dados;
 - inserção e modificação de registros de vistoria, sinistros, laudos e evidências digitais;
 - transações financeiras do Detran Pay;
 - movimentações de identidades digitais e perfis de acesso;
 - chamadas de APIs e fluxos de interoperabilidade.
Tais registros devem conter data/hora, usuário, origem, ação realizada, parâmetros relevantes e resultado da operação.
- Rastreabilidade ponta a ponta de informações sensíveis, assegurando que cada operação — desde a captura em campo até a disponibilização nos sistemas finalísticos — possa ser acompanhada de forma íntegra, contínua e detalhada. Isso é indispensável para processos como:
 - fiscalização veicular;
 - auditoria de vistorias;
 - registro e apuração de sinistros;
 - provas práticas;
 - reconciliação financeira e split de pagamentos;
 - gestão de identidades e acessos.
A rastreabilidade deve abranger a totalidade do ciclo de vida da informação.
- Capacidade de reconstrução de eventos, operações e fluxos sistêmicos para fins de auditoria, responsabilização e controle, incluindo a possibilidade de:
 - reconstituir sequências de ações realizadas por usuários ou sistemas;
 - identificar a origem de inconsistências ou divergências;
 - validar a integridade de evidências digitais;
 - correlacionar registros de múltiplos sistemas;
 - fornecer subsídios para análise de incidentes ou irregularidades.
A reconstrução deve ser tecnicamente possível, auditável e juridicamente válida.
- Geração estruturada de relatórios, evidências e informações compatíveis com as exigências de órgãos de controle e instâncias de governança, incluindo:
 - relatórios para corregedorias, controladorias e auditorias internas;
 - evidências detalhadas e exportáveis para tribunais de contas e ministério público;
 - documentação de rastros, logs e trilhas de auditoria;
 - relatórios gerenciais para comitês de governança digital e de segurança.
A solução deve simplificar a extração dessas evidências, garantindo autenticidade e integridade.

Finalidade Estratégica do Requisito

Esse requisito é essencial para:

- assegurar conformidade legal e regulatória em todas as operações;
- garantir transparência e confiabilidade dos processos do DETRAN-SP;
- permitir respostas qualificadas a auditorias, inspeções e fiscalizações;
- reforçar a segurança jurídica em processos de trânsito e atos administrativos;
- viabilizar governança moderna, baseada em dados e monitoramento contínuo;

- fortalecer a integridade institucional e prevenir fraudes, desvios ou manipulações.

Ao atender a esses requisitos, a solução tecnológica contribuirá decisivamente para elevar o padrão de governança de TIC do DETRAN-SP e consolidar um ecossistema digital seguro, confiável e auditável.

6.10. Suporte à evolução tecnológica contínua e mitigação de dependência tecnológica

A solução tecnológica a ser selecionada deverá garantir condições técnicas, arquiteturas e operacionais que permitam ao DETRAN-SP evoluir continuamente sua plataforma digital ao longo do tempo, preservando autonomia institucional, reduzindo riscos de dependência excessiva de fornecedores e assegurando que a modernização dos sistemas finalísticos possa ocorrer de maneira orgânica, sustentável e alinhada às inovações tecnológicas e regulatórias.

Para isso, a alternativa tecnológica deverá:

- Favorecer o uso de padrões abertos, interoperáveis e amplamente aceitos, tais como estruturas de APIs padronizadas, formatos de dados portáteis, protocolos reconhecidos internacionalmente e modelos de desenvolvimento aderentes a boas práticas consolidadas. O uso de padrões abertos reduz barreiras à integração, facilita auditorias e promove reuso e portabilidade.
- Evitar amarrações a componentes exclusivos, proprietários ou sem substitutos equivalentes, mitigando riscos de dependência indevida (lock-in) e garantindo que a Administração tenha liberdade para expandir, migrar ou substituir elementos tecnológicos sem necessidade de reescrita total dos sistemas ou elevados custos de transição.
- Permitir a inclusão gradual e planejada de novas tecnologias ao longo da vigência contratual, desde que tecnicamente justificáveis, juridicamente viáveis e compatíveis com os objetivos institucionais. Isso inclui adoção futura de:
 - inteligência artificial avançada e modelos generativos;
 - funcionalidades cognitivas e assistivas;
 - mecanismos aprimorados de biometria e validação geoespacial;
 - soluções de monitoramento inteligente e automação de processos;
 - recursos ampliados de análise massiva de dados (Big Data, ML, IA multimodal).
 A solução deve ser capaz de acompanhar a evolução tecnológica sem perda de estabilidade ou necessidade de reengenharia integral.
- Proporcionar flexibilidade arquitetural, permitindo ajustes, ampliações, modularizações ou modernizações sem comprometer a operação legada ou causar interrupções relevantes. A arquitetura deve assegurar que novos módulos, integrações ou funcionalidades possam ser incorporados com mínimo impacto sobre sistemas existentes.
- Viabilizar a realocação de cargas de trabalho entre diferentes ambientes, inclusive entre provedores diversos, ambientes híbridos ou infraestruturas multicloud, sempre que necessário por razões técnicas, estratégicas, econômicas ou de continuidade operacional. Essa movimentação deve ocorrer de forma segura, previsível e sem exigência de reconstrução total das aplicações ou alterações profundas de código.

Finalidade Estratégica do Requisito

O atendimento a esse conjunto de requisitos tem como objetivo:

- assegurar a evolutividade contínua da solução, evitando obsolescência acelerada ou dependência excessiva de componentes específicos;
- garantir autonomia técnica e estratégica ao DETRAN-SP, permitindo que a Administração ajuste seu ecossistema de TIC conforme necessidades futuras;
- preservar investimentos já realizados, favorecendo reuso, modularidade e compatibilidade entre gerações tecnológicas;
- reduzir custos e riscos de migração, evitando retrabalhos extensos ou interrupções operacionais em futuras transições;
- permitir adaptação rápida a novos cenários tecnológicos, regulatórios e operacionais, com flexibilidade e segurança.

Esse requisito é fundamental para assegurar que a solução tecnológica contratada não apenas atenda às necessidades atuais, mas também se mantenha sustentável, evolutiva e alinhada ao futuro digital do DETRAN-SP.

6.11. Requisitos de documentação, transferência de conhecimento e capacitação

A solução tecnológica a ser selecionada deverá assegurar que o DETRAN-SP detenha domínio técnico, operacional e gerencial sobre o funcionamento dos sistemas desenvolvidos, reduzindo dependências externas e fortalecendo a governança interna. Para isso, devem ser observados requisitos mínimos relacionados à documentação, transferência de conhecimento e capacitação das equipes institucionais ao longo de todo o ciclo de vida da solução.

A alternativa tecnológica deverá garantir, no mínimo:

- Documentação clara, completa, padronizada e permanentemente atualizada abrangendo:
- arquitetura lógica e física da solução;
- modelos de dados, fluxos de integração e topologias de rede;
- políticas de segurança da informação e controles implementados;
- rotinas operacionais, procedimentos de manutenção e diretrizes de evolução;
- regras de negócio aplicadas a cada sistema finalístico;
- manuais técnicos, funcionais e guias de uso dos componentes e APIs;
- procedimentos de contingência, recuperação e retomada operacional.
Esta documentação deve ser entregue em formato acessível, com versionamento e rastreabilidade, garantindo que alterações, correções e evoluções estejam documentadas de forma transparente.
- Transferência estruturada de conhecimento para equipes internas, incluindo processos formais de handover técnico e funcional, sessões de detalhamento arquitetural, práticas de DevSecOps, padrões de desenvolvimento, mecanismos de governança, fluxos de sustentação e gestão de ambientes.
A transferência deve ocorrer de forma progressiva, envolvendo fases de observação, operação assistida e autonomia supervisionada.
- Iniciativas de capacitação compatíveis com a complexidade, criticidade e amplitude da solução tecnológica, assegurando que servidores e equipes técnicas:
 - dominem o uso das ferramentas e componentes essenciais;
 - compreendam as políticas de segurança e boas práticas operacionais;
 - tenham condições de administrar ambientes híbridos ou multicloud;
 - acompanhem evoluções tecnológicas, integrações e procedimentos de auditoria;
 - estejam aptos a operar, monitorar e ajustar a solução em situações reais de campo.
- Mecanismos que reduzam a dependência de suporte externo, garantindo que o DETRAN-SP possa realizar atividades rotineiras, operacionais e estratégicas sem prejuízo da operação ou da continuidade dos serviços. Isso inclui:
 - autonomia para ajustes configuráveis;
 - capacidade interna de monitoramento e troubleshooting;
 - entendimento pleno da arquitetura;
 - acesso a manuais e playbooks de sustentação;
 - condições de incorporar evoluções e parametrizações sem intervenção constante do fornecedor.

Finalidade Estratégica do Requisito

O cumprimento desse conjunto de critérios é essencial para:

- fortalecer a autonomia técnica e decisória do DETRAN-SP;
- evitar dependência excessiva de fornecedores e preservar a continuidade institucional;
- assegurar governança de longo prazo sobre dados, regras de negócio e fluxos críticos;
- garantir que a modernização tecnológica resulte em capacitação permanente das equipes e não apenas na implementação de novas ferramentas;
- viabilizar uma transição gradual, responsável e sustentável entre fornecedores, tecnologias e arquiteturas ao longo do ciclo de vida da solução.

Trata-se de requisito indispensável para consolidar a maturidade institucional do DETRAN-SP, assegurando que o conhecimento crítico permaneça sob domínio da Administração Pública e que a operação dos sistemas estratégicos não seja vulnerável à dependência tecnológica externa.

6.12. Aderência ao ciclo de vida da contratação de TIC

A solução tecnológica a ser selecionada deverá aderir integralmente ao ciclo de vida das contratações de TIC, possibilitando que o DETRAN-SP execute de forma estruturada e transparente todas as etapas de planejamento, especificação, execução, monitoramento, aceitação e encerramento contratual, em conformidade com o regime jurídico aplicável e com as melhores práticas de governança pública.

Nesse contexto, a solução deverá permitir, no mínimo:

- Execução dos serviços por meio de Requisições de Serviço (RS), emitidas pela Administração, contendo escopo, requisitos funcionais e técnicos, prazos, entregáveis, marcos, critérios de aceite e métricas objetivas.
Esse modelo assegura flexibilidade para priorização de demandas, alinhamento contínuo às necessidades institucionais, rastreabilidade do esforço contratado e aderência à dinâmica evolutiva dos sistemas finalísticos.
- Desmembramento obrigatório de RS com duração superior a 30 dias, mediante estruturação de marcos ou entregas mensais aferíveis.
Essa subdivisão permite o faturamento periódico, condiciona a liquidação da despesa à entrega efetiva de produtos parciais no mês de competência e garante aderência à execução orçamentária e à boa administração de recursos públicos.
- Condicionamento do pagamento à conclusão e ao aceite formal das etapas previstas na RS, mediante comprovação objetiva do atendimento integral aos requisitos técnicos, funcionais e de qualidade estabelecidos.
Esse mecanismo vincula claramente o desembolso financeiro a resultados concretos, mensuráveis e validados, reforçando previsibilidade, segurança jurídica e integridade da execução contratual.
- Adoção de métricas objetivas e verificáveis (como USN ou métricas equivalentes) para aferição dos serviços prestados, assegurando mensuração clara do esforço, proporcionalidade entre entregas e pagamentos e adequação aos parâmetros futuros da modelagem contratual.
- Acompanhamento sistemático da execução contratual, com indicadores de desempenho, qualidade, produtividade, disponibilidade e conformidade, possibilitando correções tempestivas, aplicação de medidas de saneamento e melhoria contínua dos processos.
- Gestão contratual clara e padronizada, permitindo auditoria, fiscalização e acompanhamento por múltiplas instâncias (técnica, administrativa, controle interno e externo), com total rastreabilidade de decisões, entregas, ajustes, realinhamentos e verificações.
- Planejamento e execução estruturados de eventual transição ao término da contratação, assegurando:
 - continuidade dos serviços sem interrupção;
 - transferência completa de conhecimento e documentação;
 - preservação integral de dados, evidências, logs, histórico de configurações e infraestrutura lógica;
 - desmobilização planejada e segura da solução contratada.
A transição deverá ser transparente, auditável e tecnicamente adequada, evitando risco de descontinuidade ou perda de informações.
- Aderência às boas práticas de manutenção, sustentação, atualização e evolução contínua da solução, garantindo adequação ao ambiente operacional, proteção contra vulnerabilidades, aderência às diretrizes de governança de TIC e promoção constante da qualidade e eficiência dos serviços.

Finalidade Estratégica do Requisito

O cumprimento desses requisitos garante que a contratação:

- seja plenamente controlável e auditável;
- preserve previsibilidade orçamentária e proporcionalidade entre pagamentos e entregas;
- fortaleça a responsabilidade técnica e gerencial do fornecedor;
- minimize riscos inerentes ao ciclo de vida de soluções de TIC;
- assegure transparência, governança e integridade em todas as etapas da execução;
- viabilize a continuidade e evolução contínua dos sistemas críticos do DETRAN-SP, respeitando o arcabouço legal e institucional aplicável.

Este item consolida a necessidade de alinhar a solução tecnológica à maturidade administrativa do DETRAN-SP, garantindo que a modernização tecnológica ocorra com segurança, eficiência, ordem e sustentabilidade.

7. Estimativa da demanda - quantidade de bens e serviços

A estimativa da demanda constitui etapa essencial do planejamento da contratação e fundamenta o dimensionamento da futura solução em nuvem, garantindo que os recursos tecnológicos projetados sejam suficientes para assegurar a continuidade dos cinco sistemas finalísticos críticos: Sistema de Prova Prática, Plataforma Estadual de Vistoria (PEV), Plataforma de Pagamentos e Registro de Sinistro de Trânsito (SISTRAN).

A definição da volumetria foi construída a partir da análise combinada de múltiplos fatores operacionais, técnicos e estratégicos, assegurando que a infraestrutura contratada seja capaz de atender às necessidades presentes e projetadas, com margem adequada para expansão, resiliência e continuidade operacional.

A estimativa de consumo em USN (Unidade de Serviço de Nuvem) reflete:

- a volumetria atual e projetada dos sistemas críticos;
- a previsão de crescimento das demandas digitais;
- a interdependência entre plataformas;
- a necessidade de atender requisitos de alta disponibilidade e resiliência;
- a manutenção da eficiência operacional, especialmente em contextos de grande variação de carga;
- os registros históricos de utilização identificados em contratos anteriores;
- as especificações técnicas consolidadas nos itens 4, 5 e 6 deste ETP.

A estimativa aqui apresentada observa os princípios da economicidade, proporcionalidade, suficiência e aderência às necessidades institucionais, conforme diretrizes de planejamento previstas na Lei nº 14.133/2021 e normativos específicos de TIC.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA	
				MENSAL	TOTAL (PARA 12 MESES)
1	Sistema de Prova Prática				
1.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	2.520,1808	30242,1696
1.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	554,4398	6653,2773
1.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12
1.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12
2	Plataforma Estadual de Vistoria (PEV)				
2.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	14469,9066	173638,8792
2.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	3183,3795	38200,5534
2.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12
2.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12

3 Plataforma de Pagamento (DETRAN PAY)

3.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	5121,7813	61461,3756
3.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	1126,7919	13521,5026
3.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12
3.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12

4 Registro de Sinistro de Trânsito (RST)

4.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	3312,8454	39754,1448
4.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	728,8260	8745,9119
4.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12
4.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12

Outro fator determinante é a necessidade de adotar arquitetura em nuvem resiliente, que exige replicação entre ambientes, redundância geográfica e mecanismos de continuidade que não estavam plenamente contemplados no modelo anterior. A estratégia atual prevê ambientes de contingência, duplicação de cargas críticas, distribuição inteligente de workloads entre provedores e mecanismos automatizados de recuperação de desastres (DR), todos fundamentais para garantir a continuidade dos serviços públicos digitais em níveis compatíveis com sua essencialidade.

Somam-se a isso práticas robustas de segurança da informação, LGPD, governança de identidades (IAM) e registro de trilhas de auditoria, que aumentam o consumo de recursos como criptografia, logs, monitoramento, observabilidade e controle unificado — demandas que cresceram exponencialmente com a expansão do uso digital e com a introdução de sistemas que tratam dados sensíveis, biométricos, financeiros e evidenciais.

A estimativa considera, de forma mais precisa, picos operacionais, ambientes de homologação e testes, e demandas de sincronização offline/online para operações de campo.

A estimativa foi elaborada considerando a Memória de Cálculo (documento anexo).

8. Levantamento de soluções

O levantamento de mercado tem por finalidade identificar, analisar e comparar as alternativas de base tecnológica e serviços gerenciados capazes de atender aos requisitos de desenvolvimento e sustentação dos sistemas finalísticos críticos do DETRAN-SP. A análise considera a complexidade operacional, a criticidade dos sistemas (Prova Prática, PEV, Pagamentos, RST), a volumetria de dados, os requisitos de continuidade do serviço público e as restrições normativas aplicáveis à contratação de soluções de TIC.

Foram avaliadas soluções de ambiente para execução dos sistemas disponíveis no mercado, incluindo provedores globais (Hyperscalers), integradores especializados, plataformas de serviços gerenciados e alternativas internas da Administração Pública estadual. A análise incluiu aspectos de desempenho, segurança, conformidade, governança, escalabilidade, integração, maturidade tecnológica, modelo de custeio, riscos operacionais e aderência aos requisitos de engenharia e funcionalidade descritos no ETP.

8.1. Mercado de Computação em Nuvem Pública (Hyperscalers)

O mercado nacional e internacional de computação em nuvem é dominado por provedores de grande porte (Hyperscalers), como:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

- Microsoft Azure

Essas plataformas fornecem serviços robustos de infraestrutura (IaaS), plataforma (PaaS) e tecnologias avançadas (IA/ML, geolocalização, big data, serverless). Atendem aos requisitos de elasticidade automática, escalabilidade ilimitada, resiliência geográfica e segurança de nível corporativo. Esses recursos são indispensáveis para o desenvolvimento e execução de sistemas como o RST (com IA Generativa), Prova Prática (com Georreferenciamento e IA Multimodal) e PEV (com Big Data).

Entretanto, operar diretamente com múltiplos Hyperscalers exige elevado grau de especialização técnica, gestão permanente de ambientes heterogêneos, práticas estruturadas de FinOps e mecanismos de governança unificada — elementos que aumentam substancialmente os riscos operacionais caso não haja um integrador especializado ou serviço gerenciado capaz de absorver tais responsabilidades.

8.2. Integradores e Serviços Gerenciados de Nuvem (Multicloud Managed Services)

O mercado privado também oferece integradores especializados em operar ambientes Multicloud, realizando:

- governança unificada de múltiplas nuvens;
- automação de provisionamento e operação (DevOps / CloudOps);
- observabilidade, segurança e LGPD;
- otimização contínua de custos (FinOps);
- implantação de ambientes de DR e alta disponibilidade;
- arquitetura distribuída entre múltiplos provedores.

Apesar da expertise, essas empresas operam sob modelo comercial baseado em margem de lucro privada, com custos elevados para serviços especializados. Além disso, usualmente dependem de contratos de longo prazo e têm variação significativa de preço conforme o consumo, o que exige mecanismos complexos de fiscalização e controle contratual.

Também se observa que esse modelo mantém maior dependência tecnológica de fornecedores privados, além de envolver concorrência entre múltiplos prestadores, que nem sempre conhecem o ecossistema tecnológico específico do Estado de São Paulo.

8.3. Alternativas Internas da Administração Pública

Foram avaliadas alternativas internas existentes, notadamente a Companhia de Processamento de Dados do Estado de São Paulo (PRODESP), responsável pela infraestrutura tecnológica estruturante do Governo de São Paulo e que possui atuação direta nos sistemas essenciais do DETRAN-SP.

A PRODESP oferece serviços gerenciados de computação em nuvem Multicloud, incluindo:

- gerenciamento unificado de AWS, Azure e GCP;
- governança integrada de segurança, IAM e LGPD;
- integração com sistemas legados e finalísticos;
- automação de provisionamento e orquestração;
- práticas consolidadas de FinOps aplicadas ao setor público;
- suporte operacional aderente às normas estaduais;
- capacidade de absorção de riscos tecnológicos e operacionais;
- conhecimento histórico do arcabouço tecnológico do DETRAN-SP.

8.4 Análise Comparativa das Alternativa

Alternativa Avaliada	Pontos Fortes	Limitações / Riscos
Hyperscalers diretamente (AWS, GCP, Azure)	Máxima capacidade técnica, elasticidade, IA/ML, segurança	Elevado nível de complexidade para gestão; risco de lock-in; ausência de governança integrada; maior risco operacional

Integradores privados	Especialização, suporte técnico, serviços gerenciados	Custo elevado, desviando recursos do investimento em Engenharia de Software. Risco de dependência de fornecedor privado, com potencial dificuldade de reversibilidade, afetando a transferência de sustentação final para a PRODESP. Integração limitada com sistemas legados e históricos do DETRAN-SP, dificultando o desenvolvimento de sistemas interconectados
Solução interna – PRODESP	Expertise nos sistemas do DETRAN e arquitetura do Estado, facilitando a integração e a evolução dos novos sistemas. Governança pública e aderência integral às normas estaduais (Segurança/LGPD), crucial para o desenvolvimento de software seguro. Vantajosidade econômica, liberando recursos para o Desenvolvimento e Sustentação. Maior estabilidade operacional, com suporte institucional contínuo, garantindo o ambiente de execução dos sistemas.	Capacidade vinculada ao planejamento estadual; necessidade de alinhamento interinstitucional.

8.5. Convergência para a Solução Mais Adequada

A análise realizada convergiu para a conclusão de que a contratação de Serviços de Desenvolvimento de Sistemas utilizando a PRODESP, como entidade executora da Administração Pública Indireta, representa a alternativa mais vantajosa, eficiente e segura para o DETRAN-SP.

O foco da contratação é o desenvolvimento dos quatro sistemas essenciais (Prova Prática, RST, PEV e DETRAN Pay). O sucesso desse desenvolvimento depende de uma base tecnológica escalável e resiliente (o ambiente de nuvem), mas, acima de tudo, do conhecimento arquitetural e da integração com os sistemas já existentes.

O ciclo de vida planejado para os sistemas reforça a escolha: a contratada será responsável pelo desenvolvimento e sustentação inicial, mas, após o aceite do desenvolvimento e encerramento desse contrato, a sustentação passará integralmente para o contrato de serviços de TI que o DETRAN-SP já mantém com a PRODESP.

A escolha da PRODESP se justifica pelos seguintes diferenciais estratégicos para o desenvolvimento:

a) Domínio Institucional e Integração Arquitetural (Diferencial Crítico)

A PRODESP detém conhecimento profundo e histórico dos sistemas estruturantes, das integrações e da arquitetura tecnológica que suporta os serviços do DETRAN-SP. Este conhecimento é um diferencial importante e estratégico, pois:

- **Facilita a Engenharia de Integração:** Os novos sistemas precisam se comunicar com sistemas legados e corporativos desenvolvidos e sustentados pela PRODESP (sistemas de CNH, de Veículos, de Arrecadação). O conhecimento arquitetural prévio da PRODESP e a sua capacidade de integração nativa reduzem drasticamente a complexidade, o tempo e os riscos inerentes ao desenvolvimento, implantação e à futura evolução dos sistemas.
- **Continuidade da Sustentação:** A familiaridade da PRODESP com a arquitetura dos sistemas e com as bases de dados e APIs do DETRAN-SP garante a continuidade operacional sem "quebra" no suporte após a conclusão do desenvolvimento.

b) Conformidade Técnica e Governança Pública

O desenvolvimento dos sistemas exigirá a plena utilização de um ambiente tecnológico moderno (nuvem) para atingir os requisitos de resiliência e escalabilidade. O ambiente gerenciado pela PRODESP garante a conformidade técnica, pois:

- **Padronização:** Assegura que o desenvolvimento gere soluções que serão sustentáveis e compatíveis com o ambiente de produção do Estado de São Paulo.

- Governança de Segurança: Centraliza a governança de segurança, LGPD e FinOps para o ciclo de desenvolvimento (Dev, Homologação) e produção, essencial para o desenvolvimento de sistemas financeiros (Detran Pay) e de dados sensíveis.

c) Vantajosidade Econômica e Mitigação de Riscos

As contratações entre órgãos públicos possibilitam custos estruturados e previsíveis, sem margens comerciais privadas. Além disso, a centralização da gestão do ambiente de execução na PRODESP transfere riscos operacionais e tecnológicos para uma entidade pública com competência reconhecida, permitindo que o DETRAN-SP se concentre na gestão da funcionalidade e qualidade do desenvolvimento de software.

8.6. Conclusão do Levantamento

Diante das alternativas avaliadas, a solução de Desenvolvimento de Sistemas Críticos com Sustentação Gerenciada via PRODESP configura-se como a opção mais alinhada às necessidades técnicas, institucionais, operacionais e econômicas do DETRAN-SP. A solução é a única que garante o ambiente de execução ideal para o desenvolvimento e, simultaneamente, assegura o planejamento de sustentação de longo prazo para os sistemas críticos recém-desenvolvidos.

A solução apresenta aderência plena aos requisitos identificados nos itens 4, 5, 6 e 7 deste ETP, mitigando riscos, fortalecendo a governança e proporcionando continuidade ao processo de modernização digital do órgão.

9. Análise comparativa de soluções

A análise comparativa tem como finalidade avaliar, de forma técnica, objetiva e fundamentada, as alternativas de ambiente de execução e sustentação identificadas no levantamento de mercado. A avaliação considera a aderência dos modelos à necessidade institucional de Desenvolvimento de Sistemas Críticos (Prova Prática, PEV, RST, Pagamentos), bem como os requisitos de engenharia, os riscos operacionais, a economicidade e a governança da base tecnológica que irá hospedar esses sistemas.

Para fins de comparação, foram consideradas três categorias de solução de base tecnológica para a execução dos sistemas:

1. Contratação direta de provedores de nuvem pública (Hyperscalers).
2. Contratação de empresas privadas integradoras de serviços Multicloud.
3. Solução pública de Serviços Gerenciados Multicloud via PRODESP.

A análise foi realizada com base nos seguintes critérios:

- Capacidade técnica e performance (essencial para cargas de IA/ML e Georreferenciamento).
- Escalabilidade e elasticidade (indispensável para o autoscaling dos microsserviços).
- Governança e operação integrada Multicloud (necessária para o ambiente de execução dos sistemas).
- Segurança da informação e LGPD.
- Conformidade normativa e requisitos públicos.
- Custos e previsibilidade orçamentária.
- Dependência tecnológica e risco de lock-in.
- Integração com sistemas legados e finalísticos (crucial para a evolução dos sistemas).
- Continuidade, resiliência e mitigação de riscos.
- Aderência ao contexto institucional do DETRAN-SP.

9.1. Hipótese 1 – Operação direta com Hyperscalers (AWS, GCP, Azure)

Vantagens

- Pleno acesso às ferramentas de desenvolvimento: Portfólio avançado de serviços (IA/ML, Big Data, serverless, geolocalização) diretamente utilizável para a engenharia de software.
- Ambiente ideal para Cloud-Native: Alta escalabilidade, resiliência e disponibilidade global, essencial para o design de microsserviços e aplicações modernas.

- Máxima capacidade computacional disponível no mercado.

Limitações / Riscos

- Comprometimento da Gestão do Desenvolvimento: Exige equipe interna altamente especializada para administração da infraestrutura Multicloud, o que aumenta riscos ao órgão e desvia o foco da gestão e fiscalização da entrega do software.
- Risco de Lock-in no Desenvolvimento: Alto risco de lock-in tecnológico, especialmente em soluções de IA e georreferenciamento proprietárias, o que limita a portabilidade e a evolução arquitetural futura dos sistemas.
- Dificuldade de DevOps e Governança: Complexidade elevada de governança, IAM, segurança e FinOps, dificultando o ciclo de CI/CD e a auditoria dos ambientes de desenvolvimento/homologação entre provedores.
- Ausência de governança unificada entre provedores, dificultando controle e auditoria.

Conclusão parcial Alternativa tecnicamente robusta, mas inviável sem uma camada especializada de operação. Apresenta riscos elevados que inviabilizam a gestão eficiente do desenvolvimento e a sustentação contínua dos sistemas no contexto público.

9.2. Hipótese 2 – Contratação de integradores privados Multicloud

Vantagens

- Especialização técnica para operar múltiplos provedores, permitindo que o DETRAN-SP se concentre no desenvolvimento.
- Serviços gerenciados com suporte técnico contínuo.
- Redução parcial da complexidade de gestão para o órgão.

Limitações / Riscos

- Impacto na Integração de Software: Integração limitada com sistemas legados e históricos do DETRAN-SP, aumentando a complexidade e o risco do desenvolvimento de interfaces e APIs.
- Risco na Sustentação Futura: Alto risco de dependência de fornecedor privado, com dificuldade de reversibilidade ao final do contrato, impactando a transição de sustentação dos sistemas para a PRODESP.
- Custos geralmente elevados devido à margem de lucro do integrador, desviando recursos que poderiam ser alocados para o desenvolvimento de features.
- Fiscalização complexa, exigindo grande esforço administrativo da Administração.

Conclusão parcial Alternativa tecnicamente viável, porém, com maior risco econômico, menor aderência institucional e fragilidades quanto à continuidade, segurança e governança pública. Não é o modelo ideal para garantir a integração e o ciclo de vida dos sistemas planejados.

9.3. Hipótese 3 – Serviços Gerenciados de Desenvolvimento para Nuvem Pública Multicloud via PRODESP

Vantagens

- Conhecimento arquitetural para o Desenvolvimento: Conhecimento histórico dos sistemas finalísticos e da arquitetura do DETRAN-SP, facilitando a engenharia de integração e o desenvolvimento de APIs.
- Continuidade Assegurada: Integração nativa com sistemas corporativos do Estado, essencial para a transição da sustentação dos sistemas.
- Aderência integral às normas estaduais de segurança, governança, dados e LGPD, crucial para o desenvolvimento de sistemas que lidam com dados sensíveis e financeiros.
- Redução de riscos operacionais, tecnológicos e de continuidade.
- Custos baseados em tabelas públicas, sem lucro privado.

Limitações / Pontos de Atenção

- Necessidade de alinhamento entre áreas técnicas do DETRAN-SP e da PRODESP.
- Dependência da capacidade instalada e planejamento estadual (mitigada pelo modelo Multicloud).

Conclusão parcial: Apresenta maior aderência às necessidades levantadas, menor risco, melhor conformidade e maior estabilidade operacional no contexto do setor público. Fornece o ambiente de execução ideal e o know-how institucional para o desenvolvimento e garante a sustentação futura dos sistemas.

9.4. Comparação objetiva das alternativas

Critério	Hyperscalers (Operação Direta)	Integradores Privados	PRODESP (Solução Pública Gerenciada)
Capacidade Técnica (para Engenharia de Software)	Excelente	Muito boa	Muito boa
Governança Multicloud (para padronização de ambientes Dev/Prod)	Ausente	Parcial	Completa
Segurança / LGPD (Conformidade no desenvolvimento)	Requer gestão avançada	Depende do fornecedor	Aderente às normas públicas
Custo total (TCO no ciclo de vida do sistema)	Variável e volátil	Alto	Mais previsível
Integração com sistemas do DETRAN (Fator crítico para desenvolvimento)	Limitada	Parcial	Elevada
Risco de lock-in (Tecnológico / Sustentação Futura)	Alto	Médio	Baixo
Continuidade institucional (Assegurar a transferência de sustentação)	Frágil	Dependente de contrato	Elevada
Fiscalização e controle (Da execução do contrato)	Alta complexidade	Alta complexidade	Maior facilidade
Aderência ao ETP (itens 4, 5, 6, 7)	Parcial	Parcial	Integral

9.5. Conclusão da Análise Comparativa

A partir da avaliação das alternativas, conclui-se que:

- A operação direta com Hyperscalers oferece elevada capacidade técnica, mas impõe riscos significativos de governança, segurança, continuidade e especialização não condizentes com a estrutura atual do DETRAN-SP. Essa alternativa inviabiliza a gestão eficiente do desenvolvimento e a sustentação contínua dos sistemas no contexto público.
- A contratação de integradores privados reduz parcialmente a complexidade técnica, mas apresenta custos mais elevados, riscos contratuais e menor aderência às normas públicas estaduais. Este modelo não garante a facilidade de integração necessária para o desenvolvimento dos novos sistemas com o ambiente legado, nem a continuidade institucional para a sustentação.
- A solução de Desenvolvimento e Sustentação no Ambiente Gerenciado via PRODESP demonstra ser a alternativa mais alinhada aos requisitos técnicos, institucionais e econômicos. Atende plenamente às necessidades levantadas, reduzindo os riscos de integração devido ao conhecimento prévio da PRODESP sobre a arquitetura do DETRAN-SP, e promove a continuidade institucional no ciclo de vida do software.

Assim, a análise comparativa evidencia que a solução via PRODESP melhor atende aos princípios da eficiência, economicidade, segurança, continuidade, transparência e interesse público, configurando-se como a alternativa tecnicamente mais vantajosa para a Administração, pois assegura o ambiente ideal para o desenvolvimento e a sustentação futura dos sistemas.

10. Registro de soluções consideradas inviáveis

O processo de planejamento da contratação, conforme previsto no art. 18 da Lei nº 14.133/2021 e na IN SGD/ME nº 94/2022, exige a análise comparativa de alternativas tecnológicas e o registro formal das soluções descartadas, acompanhado da respectiva motivação técnica. Nesta etapa, foram avaliadas as possíveis estratégias de atendimento às necessidades levantadas nos itens anteriores, compreendendo modelos privados, públicos, híbridos e alternativas estruturais de infraestrutura e operação.

A seguir, registra-se, de forma motivada, as soluções consideradas inviáveis para atendimento ao objeto, após análise da sua aderência aos requisitos funcionais, tecnológicos, de segurança da informação, governança, economicidade e continuidade de serviço público.

10.1. Operação direta com Hyperscalers (AWS, Azure, GCP) sem camada gerenciada

A operação direta com provedores globais de nuvem pública consiste na contratação de serviços IaaS, PaaS e serviços de alto valor agregado diretamente dos Hyperscalers, cabendo ao órgão contratante realizar toda a governança, arquitetura, integrações, segurança, FinOps e continuidade dos ambientes.

Motivos da inviabilidade

- Complexidade operacional incompatível com a capacidade instalada do órgão:
Operar diretamente múltiplos provedores exige equipes de CloudOps, SecOps, FinOps, DevOps, engenharia de dados, arquitetura distribuída e segurança avançada — quadro de pessoal e maturidade operacional não disponíveis no DETRAN-SP.
- Ausência de governança Multicloud nativa:
Hyperscalers não operam ambientes de outros provedores, deixando toda a coordenação, unificação de identidade, compliance, automação e segurança sob responsabilidade exclusiva da Administração.
- Riscos elevados de lock-in tecnológico:
Serviços proprietários (IA/ML, mapas, serverless, análises geoespaciais, logs, pipelines) possuem forte aderência a plataformas específicas, dificultando migrações futuras e gerando dependência de tecnologias não padronizadas.
- Esforço contratual e fiscalizatório excessivo:
Exigiria múltiplos contratos distintos, fiscalizações paralelas, revisões de consumo, auditorias técnicas e validações contínuas extremamente complexas.
- Risco institucional elevado para sistemas críticos:
Sistemas como PEV, Prova Prática, Pagamentos, SISTRAN e INFOSIGA não podem operar com risco elevado de falhas administrativas decorrentes de operação direta de infraestrutura distribuída.

Conclusão parcial

Embora tecnicamente robusta, esta alternativa apresenta risco operacional e institucional incompatível com a criticidade dos serviços públicos executados pelo DETRAN-SP.

10.2. Hospedagem On-Premises / Expansão de Datacenter Próprio

A hipótese de manutenção ou expansão da infraestrutura local foi analisada considerando capacidade, custo, resiliência e evolução tecnológica.

Motivos da inviabilidade

- Escalabilidade insuficiente:
Sistemas como PEV, Prova Prática, exigem elasticidade imediata e capacidade de absorção de picos (autoscaling), inexistentes em datacenters físicos.
- Custos desproporcionalmente elevados:
Equipamentos, refrigeração, energia, espaço físico, licenças, segurança, pessoal técnico e renovações de ciclo tecnológico (refresh) tornam a solução economicamente inviável.
- Alto risco de indisponibilidade:
Eventos climáticos, falhas físicas, interrupções de energia e limitações estruturais de datacenter elevam o risco de parada.
A ausência de redundância geográfica real agrava o problema.
- Incompatibilidade com cargas de IA/ML, Big Data e processamento intensivo:
Soluções on-premises não acompanham a velocidade e a elasticidade necessárias às cargas modernas dos sistemas finalísticos.
- Contrariedade às diretrizes governamentais:
O Estado possui diretriz clara de priorização por serviços em nuvem e modernização digital (cloud-first), tornando a solução desalinhada ao planejamento estratégico.

Conclusão parcial

Solução descartada por restrições estruturais, alto custo e incapacidade de atender às exigências de escala e modernização.

10.3. Contratação de Integradores Privados de Serviços Multicloud

Avaliaram-se empresas privadas que operam ambientes Multicloud especializados.

Motivos da inviabilidade

- **Custo elevado e lucro privado direto:**
Os preços praticados no mercado privado incluem margens comerciais substanciais, o que compromete a vantajosidade econômica em comparação à solução pública.
- **Dependência contratual (lock-in empresarial):**
Uma vez que a governança da nuvem passa ao integrador, a Administração perde parte da autonomia operacional e fica vulnerável à dependência do fornecedor.
- **Menor aderência ao arcabouço regulatório estadual:**
Nem todos os integradores possuem processos compatíveis com o modelo de auditoria pública, exigências de governança, rastreabilidade, segurança e LGPD aplicáveis ao setor público.
- **Fiscalização contratual extremamente complexa:**
A estrutura de fiscalização, métricas, comprovações e análises de consumo torna-se significativamente mais pesada, aumentando riscos de disputa e passivos.
- **Menor conhecimento institucional sobre sistemas do DETRAN-SP:**
Interfaces críticas, integrações legadas e particularidades do ambiente estadual não são de domínio pleno do mercado privado.

Conclusão parcial

Embora tecnicamente viável, a alternativa apresenta vantajosidade inferior, riscos contratuais e dependência mais elevados, tornando-se inadequada.

10.4. Soluções de Cloud Parcialmente Gerenciada / Sem Governança Centralizada

São soluções onde o provedor ou integrador gerencia apenas parte da arquitetura, deixando a governança geral sob responsabilidade do órgão.

Motivos da inviabilidade

- Não atendem à exigência de governança Multicloud integrada, essencial para ambientes com AWS, GCP e Azure operando simultaneamente.
- Alto risco de inconsistência operacional, com regras de segurança, IAM, FinOps e provisionamento divergentes por provedor.
- Incompatibilidade com sistemas críticos, que exigem supervisão, continuidade e padronização absoluta (PEV, Prova Prática, SISTRAN, Pagamentos).
- Potencial aumento de custos, por ausência de política unificada de otimização e monitoramento.
- Dificuldade de reversibilidade e conformidade regulatória, com riscos à LGPD e auditoria.

Conclusão parcial

Solução tecnicamente insuficiente para o nível de integração e segurança demandado.

10.5. Soluções Privadas de Nuvem Proprietária (Private Cloud Fechada)

Abrange datacenters dedicados e plataformas privadas de cloud corporativa.

Motivos da inviabilidade

- Limitações de elasticidade, incapazes de atender cargas dinâmicas (TDV, PEV, Prova Prática).
- Ausência de redundância geográfica robusta.

- Custos altos para escala massiva de armazenamento multimídia (imagens e vídeos).
- Dependência tecnológica proprietária, dificultando migração futura.

Conclusão parcial

Solução não atende às exigências de escala, análise avançada e resiliência Multicloud.

10.6. Síntese Conclusiva da Inviabilidade

Após análise técnica detalhada:

- Soluções on-premises e privadas são incapazes de atender aos requisitos de escala, resiliência e modernização.
- Soluções diretas com Hyperscalers apresentam risco institucional elevado e não garantem governança.
- Integradores privados apresentam custo maior, risco contratual e menor aderência ao contexto público.
- Soluções parcialmente gerenciadas ou proprietárias não atendem plenamente aos requisitos do ETP.

Assim, todas as alternativas acima foram formalmente descartadas por inviabilidade técnica, operacional, econômica ou normativa.

11. Análise comparativa de custos (TCO)

A Análise do Custo Total de Propriedade (Total Cost of Ownership – TCO) tem por objetivo avaliar, de forma comparativa, os custos diretos e indiretos associados às alternativas de solução identificadas, considerando não apenas o valor monetário inicial, mas também os custos recorrentes, de operação, de manutenção, de evolução tecnológica, de governança e de mitigação de riscos ao longo do ciclo completo da contratação.

A metodologia adotada segue as diretrizes da IN SGD/ME nº 94/2022 e das boas práticas de planejamento de contratações de TIC, contemplando os seguintes componentes:

- Custos diretos: consumo de recursos de nuvem (IaaS, PaaS, SaaS), armazenamento, processamento e serviços auxiliares.
- Custos indiretos: gestão técnica, segurança, governança, equipes internas, compliance, monitoramento.
- Custos de continuidade e resiliência: ambientes redundantes, DR, contingência e alta disponibilidade.
- Custos de integração: desenvolvimento, migração, interoperabilidade, pipelines de dados.
- Custos de risco: potenciais perdas associadas a falhas, indisponibilidade, incidentes de segurança e lock-in.
- Custos de ciclo de vida: evolução tecnológica, ajustes contratuais, expansão da capacidade e atualizações.

A seguir, apresenta-se a análise comparativa entre as alternativas avaliadas.

11.1. TCO da Operação Direta com Hyperscalers

A operação direta com AWS, GCP e Azure apresenta custos distribuídos da seguinte forma:

Custos Diretos

- Consumo proporcional às cargas de trabalho (alta variação).
- Estimativa de custo significativamente maior para serviços avançados (IA/ML, reconhecimento facial, mapas, pipelines).
- Cobrança granular por API, por função serverless, por GB armazenado e por transação.

Custos Indiretos

- Necessidade de equipe interna altamente especializada (CloudOps, SecOps, FinOps, DevOps, engenharia de dados).
- Alto custo de operação, governança e monitoramento.

Custos de Continuidade / DR

- DR replicado entre regiões onerosas, com custos duplicados de armazenamento e processamento.

Custos de Integração

- Integrações complexas entre ambientes heterogêneos, sem unificação nativa de IAM.

Custos de Risco

- Elevado risco de lock-in tecnológico (especialmente IA/ML e geolocalização).
- Potencial custo elevado em caso de incidentes ou falhas operacionais.

Conclusão Parcial do TCO

Custo total alto.

Variabilidade significativa.

Necessidade de investimento interno elevado em equipes de alta especialização.

Maior risco financeiro derivado de picos e complexidade contratual.

11.2. TCO de Integradores Privados Multicloud

Custos Diretos

- Consumo equivalente ao dos Hyperscalers (repassé integral).
- Adição de margens comerciais, pacotes gerenciados, suporte e licenciamento.

Custos Indiretos

- Contrato de serviços especializados com alto valor por hora técnica ou por pacote de serviços.
- Fiscalização técnica e contratual mais onerosa.

Custos de Continuidade / DR

- Custos adicionais para replicação e garantia de ANS elevados.
- Dependência contratual que gera custos de transição e reversibilidade.

Custos de Integração

- Integrações adicionais podem ter custo variável e elevado.
- Falta de padronização com sistemas públicos aumenta esforço e despesa.

Custos de Risco

- Lock-in contratual.
- Riscos financeiros associados à dependência integral do integrador.

Conclusão Parcial do TCO

Custo total mais alto que operação direta.

Menor previsibilidade.

Custos adicionais significativos pela prestação de serviço gerenciado privado.

Baixa vantajosidade financeira no contexto público.

11.3. TCO da Solução Pública – Serviços de Desenvolvimento Gerenciados em Multicloud via PRODESP

Custos Diretos

- Modelo de repasse baseado em tabelas públicas, sem margens comerciais privadas.
- Consumo dos Hyperscalers tratado sob governança pública e com otimização contínua (FinOps).

Custos Indiretos

- Economia substancial pela eliminação da necessidade de estrutura interna altamente especializada.

- Governança, segurança, monitoramento e operação absorvidos pela estatal.

Custos de Continuidade / DR

- DR e contingência implementados sob modelo integrado, reduzindo custos duplicados.
- Maior eficiência por compartilhamento de infraestrutura e expertise institucional.

Custos de Integração

- Baixo custo incremental, devido ao conhecimento prévio da PRODESP sobre sistemas do DETRAN-SP.
- Reaproveitamento de pipelines, modelos e integrações existentes.

Custos de Risco

- Redução de risco contratual e tecnológico.
- Menor custo potencial decorrente de incidentes, por padrões unificados de segurança.

Conclusão Parcial do TCO

Menor custo total no ciclo de vida.

Alta previsibilidade orçamentária.

Eliminação de margens privadas e desperdícios.

Otimização contínua centralizada.

11.4. Comparação Estruturada do TCO

Componente de Custo	Hyperscalers Diretos	Integradores Privados	PRODESP
Consumo de nuvem	Alto	Alto + margem	Moderado/otimizado
Governança Multicloud	Alto custo interno	Médio/alto	Baixo (absorvido)
Segurança e IAM	Custos elevados	Custos elevados	Inclusos
FinOps	Necessidade interna	Prestado com custo alto	Prestado sem margem
DR / Contingência	Muito alto	Alto	Moderado/otimizado
Integração	Alto	Alto	Baixo
Equipe interna	Altíssima necessidade	Média	Baixa
Risco financeiro	Elevado	Médio	Baixo
Previsibilidade	Baixa	Média	Alta

Custo total no ciclo de vida	Mais alto	Muito alto	Mais baixo
------------------------------	-----------	------------	------------

11.5. Síntese da Análise de Custos

A análise comparativa demonstra que:

- Operação direta com Hyperscalers apresenta custo total elevado, grande variabilidade e forte dependência de equipe interna altamente especializada, resultando em TCO mais oneroso no longo prazo.
- Integradores privados apresentam TCO ainda maior devido às margens comerciais, custos de serviço gerenciado privado, complexidade contratual e risco elevado de dependência.
- A solução via PRODESP apresenta o menor TCO, maior previsibilidade orçamentária, menor complexidade de gestão, eliminação de margens privadas e redução expressiva de riscos.

Assim, a opção pública demonstra vantajosidade econômica, eficiência operacional e melhor aderência ao contexto institucional e às necessidades do DETRAN-SP, alinhando-se aos princípios da economicidade, eficiência e planejamento previstos na Lei nº 14.133/2021.

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na prestação de Serviços Gerenciados de Computação em Nuvem Pública, estruturados em arquitetura Multicloud, capazes de suportar, de forma integrada, contínua e resiliente, o desenvolvimento, implantação, evolução, operação e sustentação do ecossistema digital do DETRAN-SP. Trata-se de solução abrangente, orientada a ciclos contínuos de modernização tecnológica, que provê a infraestrutura, os serviços gerenciados e os mecanismos operacionais necessários para manter em funcionamento os sistemas finalísticos críticos, as plataformas corporativas e os ambientes analíticos essenciais à atuação institucional do órgão.

A solução deve assegurar a operação estável e segura de sistemas de alta sensibilidade, tais como: Sistema de Prova Prática, Plataforma Estadual de Vistoria (PEV), Plataforma de Pagamentos (Detran Pay) e Registro de Sinistro de Trânsito (SISTRAN), além de serviços corporativos transversais de identidade digital, integração, segurança, auditoria e governança.

A arquitetura Multicloud deverá proporcionar redundância, autonomia e independência tecnológica, permitindo que diferentes componentes operem em provedores distintos quando a estratégia institucional assim exigir, com plena interoperabilidade e governança centralizada.

A solução a ser contratada deverá contemplar, no mínimo, os seguintes atributos:

12.1. Modelo Arquitetural: Ambiente Multicloud Integrado e Gerenciado

A solução deverá operar sobre um Ambiente Integrado e Gerenciado, estruturado para combinar, de forma coordenada e transparente, recursos computacionais provenientes de múltiplos provedores de nuvem pública (Hyperscalers). A Contratada deverá desenvolver as soluções utilizando uma arquitetura Nativa em Nuvem (Cloud-Native), em ambiente de nuvem pública gerenciado, assegurando a integração e conformidade com as diretrizes de segurança e governança de dados do DETRAN-SP.

Esse modelo arquitetural é essencial para sustentar os sistemas finalísticos críticos do DETRAN-SP com altos níveis de disponibilidade, resiliência, otimização de custos, independência tecnológica e capacidade de evolução contínua.

O ambiente Multicloud, aliado à arquitetura Cloud-Native, deverá possibilitar, de forma nativa e orquestrada:

- Distribuição inteligente e dinâmica de cargas de trabalho entre diferentes provedores, considerando desempenho, latência, custo, disponibilidade regional, requisitos de segurança, geolocalização e características específicas de cada workload. Essa distribuição deve ocorrer de forma controlada e automatizada, assegurando balanceamento e continuidade.
- Independência tecnológica e mitigação de lock-in, evitando dependência exclusiva de qualquer fornecedor. A arquitetura deverá utilizar padrões abertos, componentes portáveis, APIs interoperáveis, contêineres, funções serverless com abstrações adequadas e mecanismos de gestão unificada que permitam mover aplicações e dados entre provedores sem necessidade de reescrita ou refatorações disruptivas.
- Continuidade operacional mesmo diante de falhas regionais, indisponibilidades setoriais ou incidentes de grande impacto, garantindo que a prestação dos serviços públicos essenciais — vistorias, provas práticas, sinistros e pagamentos — não seja interrompida. O modelo deve suportar failover entre provedores, replicação geográfica e construção de ambientes de contingência ativos ou passivos.

- Aproveitamento otimizado de custo-benefício entre provedores, permitindo que determinados componentes — como banco de dados, processamento analítico, serviços de IA, armazenamento, funções serverless ou mensageria — possam operar no provedor que ofereça performance, custo e aderência mais adequados. Isso inclui a adoção de estratégias de FinOps e mecanismos automáticos de otimização de capacidade.
- Atendimento simultâneo às demandas heterogêneas dos sistemas finalísticos, considerando:
 - processamento multimídia intensivo (PEV, SISTRAN);
 - operação offline-first e reconciliação segura (Prova Prática, SISTRAN);
 - transações financeiras e governança antifraude (Detran Pay);
 - pipelines de IA/ML e serviços cognitivos;
 - API Management unificado para integrações externas;
 - requisitos de baixa latência e alta disponibilidade para serviços de campo.

Esse modelo possibilita explorar capacidades especializadas de cada Hyperscaler (como serviços geoespaciais, IA generativa, APIs cognitivas, servidores serverless de alta escalabilidade, bancos distribuídos e ferramentas analíticas avançadas), garantindo eficiência máxima, flexibilidade operacional contínua e resiliência institucional.

12.2. Especificações Técnicas Por Sistema

12.2.1. Plataforma Estadual de Vistoria Veicular (PEV)

Categoria	Requisito /Funcionalidade Chave	Descrição Baseada nos Anexos
Arquitetura Principal	Centralização e Fonte Única da Verdade (SSOT)	A solução deve ser uma plataforma unificada e segura, construída nativamente em ambiente de nuvem pública. O principal objetivo é consolidar todos os laudos de vistoria em um único repositório de dados analíticos, eliminando a fragmentação de dados (hoje em 9 empresas distintas).
Funcionalidades	Gestão e Auditoria Avançada	Oferecer um portal de backoffice para o DETRAN-SP com funcionalidades de pesquisa por múltiplos critérios (placa, RENAVAM, etc.).
Migração de Dados	Transição e Desativação	Previsão da migração dos dados de vistorias existentes para a nova base na nuvem, com a desativação completa do sistema legado (e-Vistoria) ao final do processo.
Tecnologia de Dados	Orquestração de Dados	Utilização de ferramentas de Orquestração e Processamento de Dados para construir os pipelines de migração e ingestão contínua de dados (ETL), movendo e transformando os dados para o repositório analítico central.
Segurança e Conformidade	Controle de Acesso e Auditoria	Mapeamento de perfis funcionais (Administrador, Supervisor, Operador, Consulta) para papéis customizados no Serviço de Gerenciamento de Identidades e Acesso (IAM) da Nuvem, garantindo o princípio do menor privilégio. Todas as ações críticas devem ser registradas no Serviço de Log e Auditoria da Nuvem para trilha imutável.
Dados Multimídia	Armazenamento e Gestão	Implantação de solução em nuvem para armazenamento, gestão e acesso rápido de dados multimídia (imagens e vídeos) gerados nas vistorias, contemplando escalabilidade ilimitada (petabytes), baixa latência e criptografia.

12.2.2. Plataforma de Pagamentos e Compensação (DETRAN Pay)

Categoria	Requisito /Funcionalidade Chave	Descrição Baseada nos Anexos
Objetivo	Jornada de Pagamento Digital	Estabelecer os requisitos funcionais para a implementação da jornada de pagamento digital das vistorias veiculares, integrando o Portal DETRAN-SP ao ambiente financeiro do Banco do Brasil.
Modalidades de Pagamento	PIX e Sem Login Prévio	Viabilizar o recolhimento eletrônico das taxas por meio de PIX, sem a necessidade de login prévio do cidadão no Portal.
Tipos de Vistoria Abrangidas	Escopo Inicial	Pagamento digital deve abranger: Vistoria de Identificação Veicular, Vistoria de Segurança Veicular e Vistoria de Estrutura e Alteração Veicular. Deve contemplar também veículos sem RENAVAM (vinculados ao CPF/CNPJ).
Segurança	Rastreabilidade e Token	Cada transação do lote deverá possuir token individual, código de autenticação próprio e rastreabilidade completa.
Integrações	Bancárias e Backend	Integração com o Banco do Brasil para geração de QR Code PIX e retorno de status. Integração com a Base Estadual de Veículos (validação de RENAVAM) e com o Backoffice de Vistoria para abertura da vistoria. As APIs devem ser disponibilizadas de forma aberta a outros bancos interessados.

12.2.3. Plataforma de Prova Prática (Exame Prático)

Categoria	Requisito /Funcionalidade Chave	Descrição Baseada nos Anexos
Arquitetura Principal	Offline-First e Cloud	Solução composta por aplicativos móveis (tablets) para coleta de dados em campo e retaguarda em nuvem (SaaS) para processamento, auditoria e armazenamento seguro. Deve mitigar riscos de conectividade.
Funcionalidades Chave	Auditoria e Antifraude	Uso de autenticação biométrica facial no aplicativo móvel para gestão de exames. A solução deve garantir a imutabilidade da Prova, impedindo que o percurso, as faltas e os áudios gravados sejam alterados após o exame.
Localização	Georreferenciamento Avançado	Uso de GPS e integração com Plataforma de Mapas Corporativos para garantir a Auditoria Geoespacial e a certeza de que o veículo esteve na baliza oficial durante o exame.
Resiliência	Operação em Zonas de Sombra	A solução deve ter capacidade de realizar exames em locais remotos sem dependência de internet ativa (resiliência operacional).
Segurança da Informação	Criptografia Local	O banco de dados local do dispositivo (tablet) deve ser criptografado com chaves rotacionadas (ex: utilizando mecanismo de criptografia de banco de dados móvel) para impedir a extração de dados em caso de perda ou furto. Implementação de Firewall de Aplicação Web (WAF) na nuvem com regras de geobloqueio para acesso administrativo.

12.2.4. Plataforma Inteligente de Registro de Sinistros de Trânsito (RST)

Categoria	Requisito /Funcionalidade Chave	Descrição Baseada nos Anexos
Arquitetura Principal	Cloud-Native e Offline-First	Solução que permite o registro de sinistros de trânsito em modo offline no local do acidente e utiliza Inteligência Artificial Generativa para automação de laudos.
Funcionalidades	Captura de Evidências e Croqui	Captura estruturada de evidências (fotos, áudios ou texto), construção de croqui sobre mapa do local e integração com bases oficiais (veículos, CNH, CPF).
Inteligência Artificial (IA)	Automação e Análise de Montagem	Uso de mecanismos de IA para transcrever e interpretar as narrativas e condições do evento, gerando analytics estruturados. O sistema deve ser capaz de realizar o cálculo automático da montagem conforme CONTRAN, com validação de montagem.
Recursos Humanos	Perfil da Equipe	A execução exigirá equipe técnica multidisciplinar (Squad) com perfis sêniores, incluindo: Arquitetos de Soluções em Nuvem, Engenheiros de Dados e IA (Especialistas em Plataformas de Linguagem e IA), e Desenvolvedores Mobile (Especialistas em Offline-First/Sincronização).

12.3. Infraestrutura Computacional e Plataforma (IaaS/PaaS)

A solução a ser contratada deverá disponibilizar um conjunto abrangente e integrado de recursos de Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS), capaz de atender às necessidades específicas de processamento, armazenamento, comunicações, inteligência analítica e resiliência operacional dos quatro sistemas finalísticos críticos do DETRAN-SP.

O ambiente deve operar com elasticidade, segurança reforçada, observabilidade nativa, governança unificada e otimização contínua de custos, assegurando plena aderência aos requisitos funcionais e não funcionais identificados neste Estudo Técnico Preliminar.

Os componentes mínimos são descritos a seguir:

a) Computação – Elasticidade, Modularidade e Alta Performance

A infraestrutura computacional deve contemplar mecanismos avançados para alocação e gerenciamento de capacidade, incluindo:

- Instâncias elásticas com autoscaling horizontal e vertical, garantindo alocação dinâmica de CPU, memória e rede conforme a demanda real, preservando performance mesmo em picos operacionais (ex.: sincronização massiva da Prova Prática ou processamento multimídia da PEV).
- Ambiente de containers com orquestração (Kubernetes ou equivalente), permitindo modularização dos serviços, isolamento de cargas críticas e rápida implantação de novas versões, favorecendo práticas modernas de DevSecOps.
- Funções serverless de alta intensidade, essenciais para rotinas episódicas e de grande volume, como análise de imagens, transcrição automática, triggers de auditoria, cálculo de rotas e compactação de evidências digitais.
- Processamento distribuído para cargas analíticas e pipelines de dados, suportando:
 - análises geoespaciais;
 - processamento de multimídia (vídeo, imagens, áudio);
 - inferência de modelos de IA/ML;
 - validações de biometria e telemetria;
 - classificação e priorização de eventos do SISTRAN.

Esses componentes devem operar de forma integrada, com isolamento lógico entre ambientes (DEV, HMG, PRD, DR) e com governança centralizada.

b) Armazenamento – Massivo, Durável, Econômico e Altamente Disponível

A solução deverá disponibilizar múltiplas camadas de armazenamento especializadas, contemplando:

- Armazenamento de objetos distribuído, otimizado para volumetria massiva de:
- fotos e vídeos de vistorias (PEV),
- trilhas de prova prática,
- registros de sinistros e multimídia evidencial,
- telemetria e logs de observabilidade.
- Bancos de dados relacionais e não relacionais, com replicação geográfica e opções serverless, permitindo escalabilidade automática para transações críticas, cache, filas, catálogos e dados operacionais estruturados.
- Camadas de arquivamento de baixo custo (cold e deep archive), adequadas à guarda prolongada de:
- laudos,
- registros históricos,
- evidências jurídicas,
- trilhas auditáveis.
- Políticas automatizadas de ciclo de vida de dados, permitindo movimentação inteligente entre classes de armazenamento conforme tempo, criticidade, frequência de uso e requisitos regulatórios.

A arquitetura deve preservar durabilidade, integridade e capacidade de restauração, inclusive para cenários de recuperação de desastres.

c) Plataformas Especializadas – Inteligência, Governança e Processamento Avançado

A solução deverá disponibilizar serviços especializados de plataforma (PaaS) que viabilizem capacidades avançadas exigidas pelos sistemas finalísticos, tais como:

Inteligência Artificial e Machine Learning

- serviços de IA/ML para análises preditivas, auditoria cognitiva, classificação automática, transcrição de áudio, detecção de anomalias e reconhecimento de padrões;
- ferramentas para treinamento, tuning, implantação e monitoramento de modelos.

Big Data e Processamento Analítico

- plataformas de Big Data para ingestão, transformação, catalogação e análise de grandes volumes de dados estruturados e não estruturados;
- integração nativa com Data Lakes e Data Warehouses corporativos.

Serviços Geoespaciais

- geocodificação, geofencing, snapping de rotas e trilhas auditáveis;
- validação geoespacial para Prova Prática e SISTRAN, garantindo segurança jurídica e rastreabilidade.

Biometria e Tecnologias de Identidade

- mecanismos de biometria facial, fingerprint e verificação de liveness;
- apoio a validações offline/online integradas a IAM e fluxos antifraude.

Mensageria, APIs e Integrações

- serviços de mensageria escaláveis (Pub/Sub ou equivalente) para processamento assíncrono de eventos críticos;
- gateways de API com políticas unificadas de segurança, throttling, criptografia e auditoria;

- compatibilidade com integrações governamentais (gov.br, Sefaz, Sinesp, bancos parceiros).

d) Dimensionamento e Otimização Contínua

Os recursos deverão ser dimensionados:

- conforme demanda real de cada sistema,
- com zero superdimensionamento inicial,
- com elasticidade dinâmica para absorver picos,
- com observabilidade para permitir ajustes precisos (FinOps),
- com políticas automáticas de redução de capacidade em horários de baixa utilização.

O objetivo é garantir máxima eficiência técnica e financeira, preservando performance, resiliência e governança.

Essa infraestrutura IaaS/PaaS constitui o núcleo tecnológico da solução a ser contratada, assegurando que todos os sistemas finalísticos do DETRAN-SP operem com estabilidade, segurança, escalabilidade, auditabilidade e capacidade de evolução contínua, conforme diretrizes estabelecidas neste ETP.

12.4. Governança Integrada: Cloud Brokerage e Operação Unificada

A solução deverá incorporar uma camada de Cloud Brokerage plenamente integrada ao ambiente multicloud, responsável por estabelecer um modelo unificado de governança, segurança, operação e controle sobre todos os provedores de nuvem utilizados pelo DETRAN-SP. Essa camada é essencial para assegurar disciplina técnica, coerência arquitetural, observabilidade completa e autonomia institucional frente a múltiplos ambientes e fornecedores.

Essa camada deverá permitir, no mínimo:

- Gerenciamento simultâneo e centralizado dos provedores AWS, Azure, GCP (ou outros), com visão única de recursos, políticas, fluxos, métricas, serviços, identidades, custos e ativos distribuídos, garantindo que a complexidade do ambiente multicloud seja abstraída e controlada pela Administração.
- Padronização das políticas de identidade, acesso e segurança (IAM unificado), assegurando que:
- perfis, papéis, políticas, credenciais, segredos e chaves sejam geridos com consistência entre provedores;
- requisitos de segregação de funções e least privilege sejam aplicados uniformemente;
- práticas de autenticação forte, MFA e controle contínuo de acesso sejam sustentadas de forma homogênea.
- Governança baseada em políticas codificadas (policy-as-code), permitindo:
- auditoria sistematizada de conformidade;
- aplicação automática de regras de segurança, tagging, compliance, logs, criptografia, localização de dados e proteção contra exposição indevida;
- prevenção e correção instantânea de desvios de configuração (auto-remediation).
- Centralização de logs, telemetria, métricas, rastros e observabilidade, consolidando informações provenientes de:
- Prova Prática,
- PEV,
- Detran Pay,
- SISTRAN,
- serviços de integração,
- APIs expostas a terceiros,
- ambientes de desenvolvimento, homologação, produção e contingência.

A solução deverá permitir correlação de eventos entre provedores, reconstrução de fluxos, rastreamento detalhado e geração de evidências para órgãos de controle.

- Monitoramento de ANS, SLOs, SLIs e indicadores operacionais, incluindo:

- latência, throughput, disponibilidade;
- funcionamento de pipelines críticos;
- performance de sincronização offline/online;
- consumo de recursos e tendências de utilização;
- alertas preditivos para incidentes operacionais.
- Gestão integrada de custos e práticas de FinOps multicloud, assegurando:
- comparação de preços e oportunidades entre provedores;
- distribuição inteligente de workloads (right-sizing e autoscaling orientado a custo);
- detecção automática de desperdícios e anomalias de consumo;
- relatórios orçamentários claros para tomada de decisão.

Finalidade Estratégica da Camada de Cloud Brokerage

A adoção dessa camada garante que o ambiente multicloud seja:

- Padronizado, com políticas consistentes em todos os provedores;
- Auditável, com logs, eventos, métricas e rastros unificados e íntegros;
- Seguro, com controle centralizado de acessos, criptografia e conformidade;
- Resiliente, com failover entre nuvens e orquestração coerente de cargas;
- Eficiente, com otimização financeira automatizada e baseada em evidências;
- Moderno, alinhado às práticas avançadas de governança digital e ao modelo de Administração Pública Digital.

12.5. Segurança da Informação e Conformidade Legal

A solução a ser contratada deve observar, de forma estrita e inegociável, os requisitos de Segurança da Informação aplicáveis à Administração Pública, garantindo que todos os componentes da arquitetura — infraestrutura, plataformas, aplicações, integrações, serviços gerenciados e operações de campo — estejam protegidos por mecanismos robustos, auditáveis e consistentes entre múltiplos provedores de nuvem.

Tais requisitos devem assegurar que o DETRAN-SP mantenha governança plena sobre dados sensíveis, garantindo integridade operacional, segurança jurídica e conformidade regulatória.

A solução deverá garantir, no mínimo:

a) Segregação lógica e protegida dos ambientes críticos

A separação entre produção, homologação, desenvolvimento e ambientes de contingência (DR) deve ser absoluta, abrangendo:

- redes isoladas e políticas específicas por ambiente;
- segregação de identidades, permissões e grupos funcionais;
- barreiras técnicas que impeçam vazamento de dados entre ambientes;
- impossibilidade de acesso direto a dados sensíveis em DEV/HMG, com mascaramento obrigatório.

b) Criptografia ponta a ponta com padrões avançados

A solução deve adotar criptografia:

- em trânsito (TLS moderno, conforme padrões de hardening);
- em repouso (chaves gerenciadas por HSM ou KMS auditável);
- no dispositivo, no caso de operações offline em campo (ex.: SQLCipher ou equivalente);
- com rotação periódica de chaves e segregação por tipo de dado.

Esses mecanismos devem ser auditáveis, verificáveis e consistentes em todos os provedores multicloud.

c) Gestão centralizada de identidade e acesso (IAM Unificado)

A solução deverá implementar:

- autenticação forte (MFA, biometria, chaves de acesso restritas);
- política uniforme de privilégios mínimos (least privilege) e Zero Trust;
- segregação de funções críticas (SoD) em todas as camadas;
- controle granular de acesso a APIs, bancos de dados e consoles administrativos;
- inventário e rastreamento completo de identidades humanas e de máquina.

Essa governança deve permanecer unificada mesmo em ambientes multicloud.

d) Arquitetura Zero Trust e políticas de Privilégio Mínimo

A solução deve operar sob o pressuposto de que nenhum usuário, componente ou serviço é confiável por padrão. Assim:

- todas as requisições devem ser autenticadas e autorizadas;
- verificações contínuas de contexto e risco devem ser aplicadas;
- superfícies de ataque devem ser reduzidas com segmentação e microsegmentação;
- configurações seguras e padrão mínimo de hardening devem ser avaliados continuamente.

e) Proteções avançadas contra ameaças

A solução deverá incorporar mecanismos para prevenção, detecção e resposta, incluindo:

- anti-DDoS nativo e distribuído;
- proteção contra comportamento anômalo, malware, bots e exploração de APIs;
- análise e correlação contínua de logs (SIEM/SOAR);
- monitoramento de integridade de configurações e auto-remediação;
- proteção de borda com WAF, regras geoespaciais e filtragem inteligente.

f) Trilhas de auditoria completas e gravação das operações sensíveis

A solução deverá registrar com granularidade:

- ações administrativas, alterações de configuração, acessos privilegiados;
- chamadas de APIs, integrações, transações e modificações de dados;
- operações relacionadas a vistorias, sinistros, provas práticas e pagamentos;
- reconstrução de trajetórias geoespaciais e sincronizações offline.

Sessões administrativas devem ser gravadas, armazenadas de forma imutável e disponíveis para auditoria interna e externa.

g) Conformidade plena com a legislação e com normativos institucionais

A solução deverá atender integralmente:

- à Lei Geral de Proteção de Dados (LGPD), com mecanismos de anonimização, pseudonimização e controle de acesso;
- às políticas e normas estaduais de segurança da informação e privacidade;
- às exigências regulatórias aplicáveis a dados biométricos, geoespaciais, evidenciais e financeiros;
- às diretrizes institucionais de governança digital e controle estatal.

A solução deve garantir que o tratamento de dados pessoais — especialmente biométricos, geoespaciais, financeiros e evidências digitais — ocorra de forma segura, rastreável e juridicamente protegida.

h) Consistência entre provedores e rastreabilidade total

Todos os mecanismos de segurança devem operar de maneira homogênea, mesmo em arquitetura multicloud, garantindo:

- políticas unificadas de compliance;
- padronização de logs, criptografia e controles de acesso;
- auditorias integradas;
- rastreabilidade ponta a ponta em todas as cargas de trabalho.

Finalidade Estratégica do Requisito

Essa camada de segurança assegura:

- proteção integral do ecossistema digital do DETRAN-SP;
- conformidade legal e segurança jurídica;
- prevenção de incidentes e fraudes;
- preservação da confiança do cidadão e das instituições de controle;
- alinhamento com a maturidade exigida para sistemas essenciais de trânsito.

12.6. Continuidade, Resiliência e Recuperação de Desastres (DR)

A solução a ser contratada deverá garantir níveis elevados de disponibilidade, continuidade e resiliência para todos os sistemas críticos do DETRAN-SP, assegurando que falhas pontuais — sejam de infraestrutura, conectividade, provedores externos, regiões de nuvem ou componentes internos — não comprometam a prestação dos serviços essenciais ao cidadão, aos credenciados e à Administração.

A arquitetura de continuidade deverá ser projetada segundo padrões internacionais de resiliência, contemplando múltiplas camadas de redundância e estratégias robustas de recuperação de desastres, observando, no mínimo, os seguintes requisitos:

a) Arquiteturas resilientes entre múltiplas regiões e múltiplos provedores

A solução deverá operar em modelo multirregional e multicloud, garantindo que ambientes críticos estejam:

- replicados em pelo menos duas regiões distintas do mesmo provedor, ou
- distribuídos entre diferentes provedores (ex.: AWS + Azure + GCP),
- protegidos contra falhas massivas, interrupções regionais, indisponibilidades geográficas e incidentes de grande escala.

Essa distribuição deverá permitir continuidade operacional mesmo diante de eventos extremos.

b) Failover automatizado e tolerância a falhas

A arquitetura deve prever mecanismos automáticos ou semiautomáticos de:

- detecção de falhas,
- isolamento de componentes comprometidos,
- redirecionamento de tráfego,
- reinstanciação de serviços,
- failover transparente para ambientes alternativos.

Os fluxos devem ser projetados para minimizar impacto perceptível ao usuário final, inclusive em operações de campo e em rotinas de sincronização offline.

c) Ambientes completos de DR, com capacidade operacional equivalente

A solução deverá incluir um ambiente de Disaster Recovery (DR) plenamente funcional, com capacidade computacional e infraestrutura equivalentes às do ambiente primário, capaz de assumir integralmente a operação em caso de falhas.

O ambiente de DR deverá possuir:

- replicação ativa/passiva ou ativa/ativa de serviços;
- sincronização contínua ou near-real-time de dados sensíveis;
- versionamento e proteção contra corrupção ou perda de integridade;
- monitoramento independente e aferição constante de prontidão.

d) Testes periódicos de recuperação e comprovação de eficácia

A solução deverá contemplar um programa sistemático de testes, incluindo:

- simulações de falha regional,
- exercícios de failover e fallback,
- auditorias de integridade de dados e replicações,
- testes de restauração de bancos, objetos e trilhas de auditoria,
- validação de RTO (Objetivo de Tempo de Recuperação) e RPO (Objetivo de Ponto de Recuperação).

Esses testes devem ocorrer em intervalos regulares e ser documentados, possibilitando rastreabilidade por órgãos de controle.

e) Replicação de dados entre clouds para serviços estratégicos

Para garantir continuidade mesmo em incidentes graves, a solução deve incluir mecanismos de replicação inteligente de dados, tais como:

- replicação assíncrona entre múltiplos provedores;
- snapshots criptografados;
- replicação cross-region para dados críticos da PEV, Prova Prática, SISTRAN e Detran Pay;
- mecanismos antifraude que assegurem integridade, imutabilidade e cadeia de custódia dos dados replicados.

Essa replicação é fundamental para preservar evidências digitais, laudos, registros de sinistros, trilhas de prova prática e transações financeiras.

f) Autoscaling elástico para absorção de picos imprevisíveis

A solução deverá incluir autoscaling horizontal e vertical, permitindo absorção imediata de:

- picos de uso da PEV em períodos sazonais;
- cargas intensivas de processamento geoespacial no SISTRAN;
- grandes volumes de sincronizações offline de Prova Prática;
- aumento exponencial de transações em horários de alta demanda no Detran Pay.

Esse mecanismo evita indisponibilidades e degradação de desempenho.

Finalidade Estratégica do Requisito

A arquitetura de continuidade e DR deve assegurar que os serviços críticos do DETRAN-SP:

- permaneçam disponíveis de forma ininterrupta,
- resistam a falhas internas e externas,
- tenham recuperação rápida e confiável,
- preservem a integridade das informações sensíveis,

- mantenham resiliência institucional compatível com sua essencialidade pública.

Trata-se de requisito estruturante para garantir a qualidade, a segurança e a confiabilidade dos serviços digitais prestados ao cidadão paulista.

12.7. Gestão de Custos, Consumo e Otimização (FinOps)

A solução de TIC deverá incorporar um conjunto completo e integrado de práticas de FinOps Multicloud, assegurando controle granular de custos, eficiência no consumo, previsibilidade orçamentária e tomada de decisão baseada em evidências. Essa governança financeira deve permitir que o DETRAN-SP acompanhe, em tempo real, o impacto econômico das cargas de trabalho críticas — Prova Prática, PEV, SISTRAN e Detran Pay — além dos componentes corporativos, analíticos e de segurança.

A camada de gestão financeira deverá contemplar, no mínimo:

a) Dashboards unificados de consumo por sistema, ambiente e provedor

A solução deve oferecer visualizações integradas que permitam:

- análise detalhada do consumo por sistema finalístico (PEV, Prova Prática, Detran Pay, SISTRAN);
- acompanhamento por ambiente (Desenvolvimento, Homologação, Produção, DR);
- visão consolidada por provedor (AWS, Azure, GCP ou outros);
- comparação histórica de uso e identificação de tendências;
- relacionamentos entre consumo técnico e indicadores operacionais.

Esses dashboards devem ser atualizados automaticamente e permitir auditoria por centros de responsabilidade.

b) Identificação automatizada de desperdícios e ineficiências

A solução deverá detectar, de forma contínua:

- instâncias ociosas ou subutilizadas;
- volumes de armazenamento não acessados;
- funções serverless disparadas indevidamente;
- clusters superdimensionados;
- tráfego desnecessário entre provedores;
- máquinas virtuais esquecidas ou desligadas parcialmente.

A identificação deve ser automática, com sugestões de correção imediata (auto-remediation opcional).

c) Recomendações contínuas de readequação de recursos (Right-Sizing)

A solução deverá oferecer recomendações inteligentes, baseadas em:

- padrões de uso real,
- performance observada,
- sazonalidades típicas dos serviços,
- requisitos técnicos (CPU, memória, IO, throughput),
- gatilhos de segurança e compliance.

As recomendações devem permitir que o DETRAN-SP reduza custos sem sacrificar desempenho ou resiliência.

d) Projeções orçamentárias para evitar extrapolações

A solução deverá incluir mecanismos para:

- prever o consumo futuro com base em modelos preditivos;

- alertar sobre riscos de extrapolação orçamentária;
- simular crescimento de demanda (ex.: expansão da PEV, aumento de sinistros, inclusão de novos municípios);
- acompanhar a execução orçamentária mês a mês;
- recomendar ajustes antes que ocorram impactos financeiros relevantes.

Essa capacidade preserva o equilíbrio fiscal da contratação.

e) Relatórios detalhados de custos por centro de responsabilidade

A solução deverá gerar relatórios automáticos e auditáveis que permitam:

- rastrear despesas por unidade técnica, por sistema ou por diretoria;
- relacionar consumo com metas institucionais;
- justificar solicitações orçamentárias ou reforços de dotação;
- identificar cargas que geram impacto financeiro desproporcional;
- fortalecer a governança e a transparência administrativa.

Os relatórios devem ser compatíveis com exigências de controle interno e externo.

f) Políticas de desligamento automático para cargas não críticas

A solução deve permitir agendamento e desligamento automatizado de:

- ambientes de desenvolvimento e testes fora do horário comercial;
- clusters não críticos em períodos de baixa utilização;
- funções serverless que atingirem limites de consumo inesperados;
- recursos auxiliares que não impactam a operação finalística.

Esse mecanismo reduz gasto improdutivo e aumenta a eficiência operacional.

Finalidade Estratégica do Requisito

O objetivo da adoção de FinOps Multicloud é garantir:

- uso eficiente, racional e otimizado dos recursos tecnológicos;
- previsibilidade financeira, fundamental para contratações de TIC de grande escala;
- mitigação de riscos orçamentários e eliminação de desperdícios;
- alocação inteligente de custos, permitindo visibilidade plena para os gestores;
- governança financeira contínua, integrada ao ciclo de vida da contratação previsto neste ETP.

Trata-se de requisito estruturante para assegurar sustentabilidade econômica da solução e maturidade na gestão de ambientes em nuvem na Administração Pública.

12.8. Sustentação, Operação e Suporte Técnico

A solução a ser contratada deverá assegurar sustentação contínua, operação estável e suporte técnico especializado para todos os sistemas finalísticos, corporativos e analíticos do DETRAN-SP, garantindo que as aplicações permaneçam disponíveis, seguras, atualizadas e em pleno funcionamento durante todo o ciclo de vida contratual. A natureza crítica dos serviços — que envolvem operações em campo, transações financeiras, evidências digitais, sincronização offline e fluxos de auditoria — exige um modelo operacional maduro, proativo e capaz de responder rapidamente a incidentes, mudanças e evoluções tecnológicas.

A sustentação deverá contemplar, no mínimo:

a) Operação contínua 24x7 para serviços finalísticos, corporativos e de integração

A solução deve assegurar operação ininterrupta para todos os sistemas essenciais, incluindo:

- Prova Prática
- Plataforma Estadual de Vistoria (PEV)
- Registro de Sinistro (SISTRAN)
- Detran Pay
- APIs corporativas
- componentes de IAM e auditoria

A operação 24x7 deve incluir monitoramento inteligente, alertas automáticos, diagnósticos preditivos e capacidade de atuação imediata em incidentes.

b) Equipes de suporte técnico especializadas em nuvem, microsserviços e APIs

O fornecedor deverá dispor de equipes técnicas com competências específicas em:

- arquitetura multicloud;
- administração de containers e orquestração;
- DevSecOps, CI/CD e pipelines de build;
- bancos de dados distribuídos e alta disponibilidade;
- APIs e integrações de mission-critical;
- serviços geoespaciais, biometria e processamento de multimídia;
- mecanismos de cibersegurança e governança de identidades.

Essas equipes devem ser capazes de atuar em incidentes complexos e garantir o pleno funcionamento dos sistemas.

c) Atendimento e resolução de incidentes conforme ANS rigorosos

A solução deve implementar:

- SLA/SLO definidos para tempos de resposta, mitigação e solução;
- categorização de incidentes por criticidade (P1, P2, P3, etc.);
- escalonamento técnico e gerencial automático;
- comunicação estruturada com áreas técnicas do DETRAN-SP;
- mecanismos de root cause analysis (RCA) e ações de prevenção.

Incidentes que afetem Prova Prática, SISTRAN, PEV ou Detran Pay devem possuir prioridade máxima.

d) Gestão de mudanças, releases e versionamento com governança formal

A solução deverá garantir:

- processos estruturados de Change Management (ITIL/DevOps);
- cronograma contínuo de versões e releases;
- deploys automatizados com rollback seguro;
- infraestrutura para testes automatizados e validação prévia;
- rastreabilidade completa das alterações em infraestrutura, código e integrações.

Essa governança é essencial para evitar regressões ou indisponibilidades.

e) Manutenção preventiva, corretiva e evolutiva

A sustentação deverá contemplar:

- inspeções preventivas para evitar falhas futuras;
- aplicação contínua de patches e atualizações críticas de segurança;
- hardening de ambientes e reavaliação periódica de configurações;
- ajustes de performance, otimização de workloads e correções estruturais;
- suporte à evolução tecnológica dos sistemas finalísticos.

A manutenção deve ser documentada e auditável.

f) Documentação técnica completa de infraestrutura, integrações e fluxos operacionais

A solução deverá disponibilizar:

- diagramas atualizados de arquitetura multicloud;
- documentação das integrações, APIs e serviços de mensageria;
- playbooks de operação, recuperação de falhas e incident response;
- catálogos de serviços, dependências e topologias aplicacionais;
- histórico versionado de configurações, releases e mudanças.

A documentação deve ser entregue em formato acessível, versionado e atualizado continuamente.

Finalidade Estratégica do Requisito

O escopo de sustentação e operação garante que:

- os sistemas finalísticos funcionem sem interrupções,
- incidentes sejam prevenidos, mitigados e resolvidos rapidamente,
- a evolução tecnológica ocorra de maneira organizada e segura,
- a operação multicloud permaneça íntegra e confiável,
- o DETRAN-SP mantenha alta qualidade no atendimento ao cidadão e nos serviços regulatórios.

Trata-se de requisito essencial para assegurar a continuidade institucional e a confiabilidade operacional do ecossistema digital do DETRAN-SP.

12.9. Interoperabilidade e Integração com Legados

A solução a ser contratada deverá assegurar integração segura, eficiente e padronizada entre os novos componentes em nuvem e os sistemas legados atualmente em operação, garantindo continuidade dos fluxos operacionais, coerência dos dados, preservação da lógica de negócio e compatibilidade com as funções críticas do DETRAN-SP. Em um ambiente tecnológico híbrido — composto por plataformas modernas, serviços multicloud e legado on-premises — a interoperabilidade torna-se elemento essencial para evitar retrabalhos, prevenir inconsistências e permitir evolução ordenada dos sistemas.

A solução deverá atender, no mínimo, aos seguintes requisitos:

a) Interoperabilidade plena com sistemas finalísticos estratégicos

A solução deve permitir comunicação segura, estável e de baixa latência com:

- Plataforma Estadual de Vistoria (PEV), com ingestão de laudos, fotos, vídeos e trilhas técnicas;
- Sistema de Prova Prática, suportando sincronização de dados offline/online, validação biométrica e auditoria multimídia;
- Registro de Sinistro de Trânsito (SISTRAN), com validação geoespacial, telemetria e ingestão de evidências;
- Plataforma de Pagamentos (Detran Pay), garantindo integração financeira segura, registro de transações, conciliação e trilhas auditáveis;
- Sistemas corporativos, administrativos e regulatórios.

As integrações devem respeitar padrões de versionamento, disponibilidade e resiliência.

b) Ingestão contínua e padronizada de dados para o Mega Lake

A solução deverá oferecer mecanismos de ingestão automática, segura e rastreável de dados para o Mega Lake e demais camadas analíticas, incluindo:

- pipelines de ingestão em streaming e batch;
- captura e catalogação de dados estruturados, semiestruturados e não estruturados;
- enriquecimento, deduplicação e versionamento de dados;
- integração com Data Warehouse e Data Marts;
- compatibilidade com mecanismos de governança, catalogação (Data Catalog) e segurança de dados analíticos.

A ingestão deve ser contínua, imutável e auditável, permitindo análises gerenciais, inteligência institucional e tomada de decisão baseada em dados.

c) Integração com plataformas federais e serviços externos

A solução deve contemplar integrações com serviços governamentais externos essenciais, tais como:

- bases biométricas federais;
- RENAVAM e outros cadastros nacionais;
- DENATRAN ou entidades equivalentes;
- serviços geoespaciais federais;
- plataformas de autenticação e validação (ex.: gov.br);
- serviços de arrecadação e bilhetagem (bancos parceiros).

As integrações deverão observar requisitos de segurança, criptografia, segregação e controle de acesso compatíveis com dados sensíveis.

d) Funcionalidade unificada e disciplinada do ecossistema de APIs internas

A solução deverá estruturar um ambiente unificado de APIs para:

- padronizar governança de integrações;
- centralizar políticas de autenticação e autorização;
- registrar todas as chamadas, respostas e falhas (observabilidade full-stack);
- permitir evolução incremental sem quebra de compatibilidade;
- fornecer documentação atualizada via API Gateway e portais de desenvolvedores.

Essas APIs devem garantir interoperabilidade transparente entre sistemas de diferentes eras e arquiteturas.

e) Preservação da lógica de negócios e dos fluxos operacionais consolidados

A solução deverá assegurar que:

- as regras de negócio vigentes sejam preservadas, auditáveis e rastreáveis;
- os fluxos existentes não sofram interrupções, fragmentações ou regressões;
- migrações tecnológicas não imponham reengenharia desnecessária;
- os sistemas legados possam continuar operando com estabilidade enquanto coexistem com novas soluções.

Isso evita perda de funcionalidades históricas e garante continuidade institucional.

f) Integração projetada para reduzir retrabalho, duplicidade e inconsistências

As integrações deverão ser concebidas para:

- eliminar redundância de cadastros e dados;
- evitar duplicidades entre legados e novos módulos;
- minimizar necessidade de retrabalho humano;
- garantir consistência transacional entre múltiplas plataformas;
- padronizar formatos, protocolos e modelos de dados.

A arquitetura deve favorecer reutilização, centralização de informações e Fonte Única da Verdade (SSOT).

Finalidade Estratégica do Requisito

A interoperabilidade e a integração com legados garantem que:

- a modernização tecnológica ocorra de forma segura, gradual e sem rupturas;
- os sistemas finalísticos continuem operando sem interrupções;
- o DETRAN-SP preserve seu patrimônio informacional e operacional;
- a transição para a nuvem seja sustentável, coerente e alinhada à estratégia digital;
- os sistemas novos e antigos funcionem como partes de um ecossistema integrado, e não como ilhas isoladas.

Trata-se de requisito essencial para assegurar evolução contínua, governança unificada e consistência operacional em todo o ambiente digital do DETRAN-SP.

12.10. Abrangência da Solução: Portfólio de Sistemas Atendidos

A solução de TIC a ser contratada deverá atender, de forma integral, contínua e integrada, todo o conjunto de sistemas finalísticos, corporativos e analíticos que compõem o ecossistema tecnológico do DETRAN-SP. A arquitetura gerenciada, os serviços gerenciados, os mecanismos de segurança, a governança unificada e a operação 24x7 deverão suportar não apenas o funcionamento individual de cada plataforma, mas sobretudo a interdependência entre elas, garantindo desempenho, escalabilidade, resiliência, rastreabilidade e continuidade operacional em todas as frentes de atuação do órgão.

A abrangência mínima contempla os seguintes sistemas estratégicos:

a) Sistema de Prova Prática

A solução deverá assegurar infraestrutura e recursos que suportem:

- operação offline-first para aplicação de provas em campo;
- validação biométrica (1:1), trilhas geoespaciais e auditoria multimídia;
- sincronização segura e resiliente com ambiente em nuvem;
- alta disponibilidade para usuários, examinadores e credenciados;
- ingestão de dados para o Mega Lake e sistemas analíticos.

Trata-se de sistema de alta sensibilidade operacional e jurídica.

b) Plataforma Estadual de Vistoria (PEV)

A solução deverá garantir suporte completo às operações de vistoria digital, incluindo:

- upload e processamento intensivo de fotos, vídeos e metadados;
- validação de informações em tempo real;
- integração com sistemas legados de veículos e credenciados;

- mecanismos robustos de auditoria, cadeia de custódia e SSOT (Fonte Única da Verdade);
- escalabilidade automática para absorver picos sazonais de demanda.

A PEV demanda volumetria massiva, alta resiliência e governança de integridade.

c) Plataforma de Pagamentos (Detran Pay)

A solução deverá oferecer infraestrutura segura e resiliente para:

- processamento de transações financeiras;
- split, conciliação e clearing interno;
- integração com bancos parceiros e plataformas estaduais;
- mecanismos de antifraude e proteção a dados sensíveis;
- auditoria completa de transações e logs de segurança.

Por envolver dados financeiros, exige padrões avançados de segurança e continuidade.

d) Registro de Sinistro de Trânsito – SISTRAN

A solução deverá suportar:

- ingestão de dados geoespaciais, telemetria e evidências multimídia;
- reconstrução de trajetos com snapping-to-road e validação geográfica;
- auditorias inteligentes e análise multimodal (foto, vídeo, áudio, rota);
- integração com órgãos estaduais e federais;
- tratamento seguro de informações de alto impacto jurídico.

O SISTRAN exige processamento intenso, capacidade analítica e alta disponibilidade.

e) Sistemas Transversais, Corporativos e Integradores

Além dos sistemas finalísticos, a solução deverá atender todo o conjunto de módulos e componentes que sustentam o funcionamento do ecossistema digital, tais como:

- mecanismos de IAM e gestão de identidades;
- gateways de API e serviços de mensageria;
- plataformas de auditoria, logs e observabilidade;
- catálogos, bases corporativas e motores de integração;
- mecanismos de DR, backup, replicação e continuidade operacional;
- sistemas de apoio às unidades administrativas e fiscalizatórias.

Esses componentes garantem coerência, integridade e governança contínua sobre todo o ambiente.

Finalidade Estratégica da Abrangência

Ao atender integralmente todos esses sistemas, a solução assegura:

- continuidade operacional ininterrupta dos serviços essenciais;
- modernização coordenada do ecossistema tecnológico do DETRAN-SP;
- unificação de padrões técnicos e de segurança;
- redução de retrabalho e duplicidades;
- maior eficiência operacional e melhor experiência do cidadão;

- fortalecimento da governança digital e da resiliência institucional.

A abrangência descrita constitui requisito estruturante para garantir que a solução contratada suporte, de forma coesa e integrada, todo o portfólio de serviços digitais do DETRAN-SP.

13. Estimativa de custo total da contratação

Valor (R\$): 170.617.823,06

A estimativa de custo total da contratação foi elaborada a partir da consolidação das necessidades tecnológicas identificadas, das quantidades de consumo previstas e da análise comparativa das alternativas tecnológicas descritas deste ETP. A formulação considera o porte institucional do DETRAN-SP, a criticidade dos sistemas finalísticos envolvidos, a crescente complexidade do ecossistema digital e a necessidade de continuidade ininterrupta dos serviços públicos digitais ofertados pelo órgão.

A estimativa contempla a projeção de consumo dos Serviços Gerenciados de Computação em Nuvem Pública em Arquitetura Multicloud, abrangendo recursos essenciais de:

- computação elástica e processamento distribuído;
- armazenamento massivo distribuído e camadas de arquivamento;
- bancos de dados relacionais, NoSQL e serviços especializados;
- plataformas de Big Data e Inteligência Artificial;
- serviços geoespaciais, biometria e mensageria;
- mecanismos avançados de segurança, auditoria e proteção de identidades;
- ambientes completos de contingência (DR) e replicação multirregional;
- governança centralizada, observabilidade, suporte técnico e operação 24x7.

13.1. Parâmetros e Fatores Considerados

A definição da estimativa global considerou um conjunto de elementos técnicos, operacionais e estratégicos, entre eles:

a) Demandas atuais e projetadas dos sistemas finalísticos críticos

Incluindo:

- Plataforma Estadual de Vistoria (PEV) – volumetria massiva de fotos, vídeos e evidências;
- Sistema de Prova Prática – uso intensivo de sincronização offline, biometria e trilhas multimídia;
- Registro de Sinistro de Trânsito (SISTRAN) – cargas geoespaciais, telemetria e auditoria cognitiva;
- Plataforma de Pagamentos (Detran Pay) – transações financeiras, conciliação e antifraude.

b) Ampliação das cargas corporativas e de integração

Com destaque para IAM, API Gateway, mensageria, Data Lake, Data Warehouse e ferramentas de auditoria.

c) Crescimento natural da volumetria e do tráfego

Decorrente da digitalização de serviços, expansão de municípios atendidos e aumento de evidências digitais.

d) Exigências de resiliência e alta disponibilidade

Tais como:

- operações multirregionais,
- replicação geográfica,
- contingência ativa/standby,
- failover automatizado.

e) Práticas de FinOps

Com foco em:

- otimização contínua,
- eliminação de desperdícios,
- dimensionamento preciso (right-sizing),
- previsibilidade orçamentária.

f) Consideração de sazonalidades e picos operacionais

Como:

- períodos de alta demanda de vistorias;
- aumento de provas práticas em determinadas épocas;
- expansão de envio de sinistros após eventos de grande impacto;
- picos de arrecadação e uso do Detran Pay.

13.2. Metodologia Utilizada

A metodologia de estimativa combinou:

a) Levantamento de preços praticados pelos principais provedores públicos de nuvem

Considerando modelos equivalentes de:

- consumo multicloud,
- serviços gerenciados,
- replicação entre regiões,
- ambientes ativos de DR,
- plataformas de Big Data e IA.

b) Análise dos contratos e memórias de cálculo anteriores

Incluindo:

- volumes históricos efetivamente consumidos,
- curvas de crescimento dos últimos ciclos,
- previsões de uso conforme evolução dos sistemas finalísticos.

c) Projeção incremental decorrente do portfólio ampliado

Com destaque para:

- aumento de cargas multimídia (PEV e Prova Prática),
- maior dependência de análises geoespaciais (SISTRAN),
- ampliação do volume financeiro processado (Detran Pay).

d) Economia de escala obtida pela consolidação multicloud

Resultado da unificação de sistemas sob uma camada única de:

- governança,

- operação,
- FinOps,
- controle de identidades,
- monitoramento e observabilidade.

Esse fator reduz redundâncias, melhora eficiência operacional e diminui o custo marginal das cargas distribuídas.

13.3. Componentes da Estimativa de Custo

A estimativa consolidada contempla:

a) Consumo mensal de serviços de nuvem pública multicloud, incluindo:

- CPU, GPU, memória e instâncias elásticas;
- funções serverless;
- armazenamento primário, secundário e arquivamento;
- bancos de dados de alta disponibilidade;
- tráfego de rede e replicação entre provedores;
- cargas de IA/ML, Big Data e serviços multimídia.

b) Governança, operação e suporte técnico

- operação 24x7;
- sustentação dos ambientes;
- equipes especializadas em nuvem, APIs e segurança;
- observabilidade e telemetria;
- gestão de mudanças e releases.

c) Continuidade e contingência

- ambientes completos de DR;
- replicação cross-region;
- failover e fallback;
- testes periódicos de recuperação.

d) Governança financeira (FinOps)

- dashboards unificados;
- análise preditiva de custos;
- recomendações de otimização contínua;
- governança por centros de responsabilidade.

e) Evolução do portfólio de sistemas

- suporte à modernização contínua;
- ampliação dos ambientes de prova, homologação e experimentação;
- novas cargas decorrentes da Plataforma de Pagamentos e do SISTRAN.

f) Segurança da informação

- IAM unificado;

- criptografia avançada;
- WAF, DDoS e proteção de borda;
- auditoria imutável;
- tratamento seguro de dados biométricos, geoespaciais e financeiros.

13.4. Síntese e Finalidade da Estimativa

A estimativa de custo total apresenta caráter técnico, indicativo e preliminar, destinada exclusivamente a embasar o planejamento da contratação, conforme determina a legislação vigente e boas práticas de governança de TIC.

O valor final será apurado na fase seguinte, durante a apresentação das propostas, na forma definida pela modalidade de contratação, com:

- composição detalhada de preços,
- validação técnica dos insumos,
- demonstração de economicidade,
- comprovação de aderência aos requisitos do ETP e do futuro TR.

A estimativa aqui apresentada consolida os custos necessários para viabilizar a operação multicloud integrada, segura, escalável e resiliente, garantindo estabilidade e continuidade dos serviços finalísticos e corporativos do DETRAN-SP.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE ESTIMADA		VALOR	
				MENSAL	TOTAL (PARA 12 MESES)	UNITÁRIO	TOTAL (PARA 12 MESES)
1	Sistema de Prova Prática						
1.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	2.520,1808	30242,1696	R\$ 534,87	R\$ 16.175.629,25
1.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	554,4398	6653,2773	R\$ 107,53	R\$ 715.426,91
1.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12	R\$ 1.786,72	R\$ 21.440,64
1.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12	R\$ 2.656,48	R\$ 31.877,76
2	Plataforma Estadual de Vistoria (PEV)						
2.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	14469,9066	173638,8792	R\$ 534,87	R\$ 92.874.227,32
2.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	3183,3795	38200,5534	R\$ 107,53	R\$ 4.107.705,51
2.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12	R\$ 1.786,72	R\$ 21.440,64

2.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12	R\$ 2.656,48	R\$ 31.877,76
3	Plataforma de Pagamento (DETRAN PAY)						
3.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	5121,7813	61461,3756	R\$ 534,87	R\$ 32.873.845,97
3.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	1126,7919	13521,5026	R\$ 107,53	R\$ 1.453.967,17
3.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12	R\$ 1.786,72	R\$ 21.440,64
3.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12	R\$ 2.656,48	R\$ 31.877,76
4	Registro de Sinistro de Trânsito (RST)						
4.1	Consumo de Serviços em Nuvem - USN (Consumo)	27324	USN/Mês	3312,8454	39754,1448	R\$ 534,87	R\$ 21.263.299,43
4.2	Consumo de Serviços em Nuvem – USN (Gerenciado)	27324	USN/Mês	728,8260	8745,9119	R\$ 107,53	R\$ 940.447,91
4.3	Gestão de consumo em Nuvem	27324	POR MÊS	1	12	R\$ 1.786,72	R\$ 21.440,64
4.4	Conectividade para Nuvens Públicas	27324	UNIDADE/MÊS	1	12	R\$ 2.656,48	R\$ 31.877,76
TOTAL							R\$ 170.617.823,06

Os subitens 1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 4.1, 4.2 e 4.3, da tabela acima, se encontram na Tabela de Preços de Insumos de Informática (SEI nº), aprovada pela Resolução SGGD nº 17, de 13 de maio de 2024, considerando o disposto no artigo 9º do Decreto Estadual nº 67.888, de 17 de agosto de 2023.

Os subitens, 1.4, 2.4, 3.4 e 4.4, da tabela acima, foram analisados os preços através de contratos similares entre a PRODESP e outros órgãos, dessa forma comprovando que a contratada pratica os mesmos preços para outros entes da Administração Pública

14. Justificativa técnica da escolha da solução

A escolha pela solução de Desenvolvimento de Sistemas através de Serviços Gerenciados de Computação em Nuvem Pública fundamenta-se na necessidade institucional de acessar um ambiente que possibilite o desenvolvimento das funcionalidades exigidas e solucionar a obsolescência de arquiteturas legadas, conforme o ETP.

14.1. Única Via para o Desenvolvimento de Funcionalidades Críticas: O ambiente on-premise não suporta a engenharia de software demandada. O desenvolvimento exige o uso de serviços nativos de nuvem (como Vertex AI, Google Maps Platform e microsserviços serverless) para implementar: a Auditoria Geoespacial (Prova Prática), a IA Generativa (RST) e a escalabilidade elástica que garante o processamento de milhões de transações do Detran Pay e da PEV. A nuvem é o único ambiente que viabiliza o requisito Offline-First em larga escala.

14.2. Aderência ao Modelo de Pagamento por Resultados (Milestones): A contratação dos serviços de desenvolvimento por Milestones (Detran Pay, RST, PEV) exige uma metodologia ágil (DevOps) que só é plenamente suportada pela nuvem. A criação e destruição automatizada de ambientes de desenvolvimento e testes, o pipeline CI/CD (Infraestrutura como Código) e os mecanismos de observabilidade da nuvem são essenciais para que o DETRAN-SP possa atestar e aceitar tecnicamente os marcos de desenvolvimento antes do pagamento.

14.3. Mitigação de Riscos Sistêmicos de Desenvolvimento: A solução Multicloud, com o gerenciamento da PRODESP, garante que o desenvolvimento seja realizado em um ambiente com Segurança Centralizada e aderente à LGPD, incluindo a subscrição de Segurança Estratégica (Mandiant). Isso reduz o risco de inconsistências na codificação e na integração com legados. O foco no desenvolvimento Cloud-Native resolve o problema de obsolescência e fragmentação do ecossistema, estabelecendo um padrão único e evolutivo para todos os sistemas críticos do órgão.

15. Justificativa econômica da escolha da solução

A escolha da solução de Serviços Gerenciados de Computação em Nuvem Pública Multicloud, operada pela PRODESP, apresenta vantagem econômica comprovada ao otimizar o custo total de propriedade (TCO) do ciclo de desenvolvimento e sustentação de sistemas críticos. A análise econômica foi conduzida à luz do princípio da economicidade, focando em como a nuvem reduz custos associados à engenharia de software e ao desenvolvimento de funcionalidades avançadas. A justificativa econômica decorre dos fatores a seguir.

15.1. Vantajosidade Econômica no Desenvolvimento e Sustentação

A solução elimina custos indiretos significativos que, no modelo on-premise, desviariam recursos do desenvolvimento de features:

- **Redução de Custos de Squad e Especialização:** A contratação transfere para o provedor especializado a gestão operacional e a sustentação 24x7. Isso permite ao DETRAN-SP reduzir a necessidade de manter uma equipe interna altamente especializada em arquitetura CloudOps, SecOps e FinOps, liberando recursos para focar na gestão da qualidade e fiscalização dos entregáveis de software.
- **Acesso Racionalizado a Ferramentas de Engenharia:** A nuvem proporciona acesso pay-per-use a recursos caros, como IA/ML (Gemini), Big Data e serviços de Georreferenciamento, que são indispensáveis para o desenvolvimento dos novos sistemas (RST, Prova Prática). A hospedagem local desses recursos seria economicamente inviável.
- **Racionalização de Ambientes de Desenvolvimento:** O modelo Multicloud permite a criação e o descarte rápido de ambientes segregados (Dev /Homologação/Testes), alinhado ao Ciclo de Vida de Software Ágil (DevOps). Isso garante que o órgão pague apenas pelo tempo de uso dos recursos, eliminando o custo de infraestrutura ociosa.
- **Conformidade Financeira no Pagamento por Resultado:** O TCO é otimizado pelo uso do modelo de pagamento por Milestones (marcos de desenvolvimento) para os serviços de Engenharia de Software. A solução em nuvem garante a rastreabilidade e a verificação técnica (medição objetiva e Cloud Logging) necessárias para vincular o desembolso financeiro ao aceite formal da funcionalidade concluída.

15.2. Mitigação de Riscos e Ganhos de Escala (FinOps)

A opção pelo desenvolvimento na Nuvem Gerenciada otimiza o TCO ao mitigar riscos financeiros decorrentes de ineficiência e indisponibilidade:

- **Evita Custos de Retrabalho por Falha de Infraestrutura:** A Resiliência Operacional e o Offline-First dos sistemas desenvolvidos (RST, Prova Prática) evitam custos indiretos elevados, como retrabalho e paralisações, causados por falhas de conectividade ou indisponibilidade sistêmica.
- **Governança Financeira Centralizada (FinOps):** O modelo inclui práticas sistemáticas de FinOps, que proporcionam controle contínuo, eliminação de recursos subutilizados e ajustes automáticos de capacidade. Isso previne o crescimento de consumo sem governança, o que é um risco comum e oneroso em ambientes de alta elasticidade.
- **Vantagem Econômica da PRODESP:** A contratação por meio da PRODESP elimina a margem de lucro privada do integrador, resultando no menor Custo Total de Propriedade (TCO), e garante a continuidade institucional da sustentação dos sistemas desenvolvidos, reduzindo custos de transição futura.

Conclui-se que a solução é economicamente mais vantajosa porque maximiza o retorno sobre o investimento em desenvolvimento de software e mitiga riscos financeiros, alinhando-se plenamente ao princípio da economicidade.

16. Benefícios a serem alcançados com a contratação

A contratação dos serviços de desenvolvimento e modernização dos sistemas críticos, utilizando uma arquitetura Cloud-Native e uma plataforma Multicloud gerenciada (via PRODESP), tem o potencial de gerar benefícios substanciais que vão além da infraestrutura, impactando diretamente a qualidade do serviço público, a segurança jurídica e a eficiência operacional do DETRAN-SP.

16.1. Segurança Jurídica e Mitigação de Fraudes

O desenvolvimento focado em funcionalidades avançadas providas pela nuvem garantirá maior segurança jurídica e o combate efetivo à fraude.

- **Imutabilidade de Evidências:** A nova arquitetura Cloud-Native assegurará a cadeia de custódia digital e a imutabilidade de laudos, fotos, vídeos, áudios e registros de GPS, eliminando o risco de adulteração em processos críticos como Prova Prática e Registro de Sinistro de Trânsito (RST).
- **Auditoria Cognitiva (IA/Geolocalização):** O desenvolvimento permitirá a integração de Inteligência Artificial Generativa (IA Gemini) e Georreferenciamento Avançado (Geofencing/Snap-to-Road) para garantir a auditoria de trajeto, validação geoespacial de alta precisão e mitigar fraudes de conduta e geográficas na Prova Prática e no RST.
- **Trilhas de Auditoria Invioláveis:** Serão garantidas trilhas de auditoria completas e imutáveis, essenciais para a rastreabilidade integral de operações financeiras (Detran Pay), de vistoria e de sinistros, atendendo às exigências dos órgãos de controle.

16.2. Continuidade Operacional e Resiliência em Campo

O desenvolvimento dos sistemas críticos (Prova Prática, RST) com a arquitetura Offline-First resolve os gargalos operacionais causados pela dependência de conectividade, garantindo a continuidade do serviço público em campo.

- **Operação Ininterrupta:** O desenvolvimento permitirá que agentes em campo (Provas Práticas e Sinistros) possam coletar e registrar dados, biometria, áudios e fotos mesmo sem internet, eliminando paralisações e inconsistências.
- **Sincronização Segura:** Os sistemas garantirão a sincronização automática, segura e transacional dos dados assim que a conectividade for restabelecida, evitando perda de evidências e retrabalho.
- **Alta Disponibilidade Global:** A hospedagem dos sistemas desenvolvidos na arquitetura Multicloud gerenciada garantirá resiliência geográfica e DR (Disaster Recovery), mantendo os serviços essenciais contínuos e estáveis, mesmo diante de falhas amplas.

16.3. Modernização e Eficiência da Gestão Pública

O desenvolvimento de novos sistemas em ambiente Cloud-Native e a consolidação de dados promoverão a transformação digital, resultando em ganhos de eficiência e melhor gestão da informação.

- **Fonte Única da Verdade (SSOT):** O desenvolvimento da Plataforma Estadual de Vistoria (PEV) e dos demais sistemas centralizará 100% dos laudos e dados de trânsito em um repositório unificado, facilitando a fiscalização, análise avançada e o uso de inteligência de dados.
- **Aceleração de Processos:** A integração de IA Generativa no RST (Registro de Sinistro de Trânsito) permitirá a padronização de laudos e acelerará a liberação do documento ao cidadão de dias para horas.
- **Governança Financeira (Detran Pay):** O desenvolvimento da Plataforma de Pagamentos (Detran Pay) como uma Clearing House interna centralizará o split de pagamentos, garantirá conciliação em tempo real e consistência transacional (ACID), eliminando riscos críticos e processos manuais.

16.4. Otimização de Custos e Racionalidade Financeira

O modelo de contratação de desenvolvimento e hospedagem na Nuvem Pública Gerenciada (via PRODESP) otimiza o Custo Total de Propriedade (TCO) do ciclo de vida dos sistemas.

- **Uso Racional de Recursos Caros:** A nuvem permite o acesso pay-per-use a recursos caros e indispensáveis, como IA/ML (Gemini) e Georreferenciamento, que seriam economicamente inviáveis em hospedagem on-premises.
- **Eliminação de Custos Indiretos:** A gestão do ambiente (CloudOps, SecOps, FinOps) será absorvida pela entidade gerenciadora (PRODESP), liberando o DETRAN-SP de manter uma estrutura interna altamente especializada e onerosa.
- **FinOps Contínuo:** O modelo de gestão na nuvem inclui práticas robustas de FinOps, garantindo o autoscaling controlado (redução de serviços ociosos) e a otimização contínua de capacidade, o que previne o crescimento de consumo sem governança, comum em ambientes elásticos.

16.5. Mitigação de Risco e Continuidade Institucional

A escolha da solução gerenciada pela PRODESP mitiga riscos tecnológicos e contratuais e garante a evolução sustentável dos sistemas.

- **Integração Nativa:** O conhecimento arquitetural e institucional da PRODESP sobre os sistemas legados e bases de dados do DETRAN-SP facilita a engenharia de integração dos novos sistemas, reduzindo a complexidade, o tempo e os riscos do desenvolvimento.
- **Sustentação de Longo Prazo:** A familiaridade da PRODESP com a arquitetura garante a continuidade operacional sem rupturas após a conclusão do desenvolvimento, já que a sustentação final passará para o contrato que o DETRAN-SP já mantém com ela.
- **Conformidade Pública:** O desenvolvimento será realizado em um ambiente que adere integralmente às normas estaduais de LGPD, Segurança e Governança, essenciais para o tratamento de dados sensíveis e financeiros.

17. Providências a serem Adotadas

Para dar continuidade ao processo que poderá resultar na contratação da solução analisada neste Estudo Técnico Preliminar, será necessário adotar um conjunto de providências técnicas, administrativas e de governança, de modo a garantir que as etapas subsequentes sejam conduzidas com a robustez exigida pela legislação aplicável. A primeira delas consiste na elaboração detalhada do Termo de Referência, documento que deverá consolidar os requisitos funcionais, não funcionais, operacionais e de desempenho identificados neste ETP, incluindo a descrição do objeto, os níveis mínimos de serviço, as obrigações das partes, os critérios de medição e verificação, a matriz de riscos inicial e os requisitos de segurança e governança.

Paralelamente à elaboração do TR, será necessária a revisão e validação técnica do dimensionamento estimado, em articulação com as equipes envolvidas na operação dos sistemas finalísticos e corporativos, bem como com as áreas responsáveis por arquitetura, segurança e infraestrutura, de forma a assegurar que os volumes de consumo, armazenagem, capacidade computacional e requisitos de disponibilidade estejam coerentes com as necessidades institucionais. Em seguida, caberá às áreas responsáveis pelo planejamento orçamentário promover a compatibilização entre a demanda e as dotações disponíveis, realizar os ajustes necessários no Plano de Contratações Anual e assegurar a reserva orçamentária pertinente, para viabilizar o prosseguimento da instrução.

O processo deverá ser submetido também à análise jurídica, que avaliará a conformidade da modelagem de contratação, a adequação dos fundamentos técnicos, a aderência às normas da Lei nº 14.133/2021, bem como a coerência das cláusulas da minuta contratual com as obrigações previstas. Além disso, o processo deverá ser encaminhado ao COETIC, para análise da aderência ao planejamento estratégico de TIC, verificação da compatibilidade tecnológica da solução, avaliação dos riscos arquiteturais e emissão da manifestação conclusiva necessária ao prosseguimento.

Outra providência essencial é a elaboração e consolidação da matriz de riscos, contemplando riscos operacionais, tecnológicos, financeiros, contratuais e de segurança da informação, bem como as correspondentes medidas de mitigação e contingência, em conformidade com a IN SEGES nº 65/2021. Também será necessário estruturar os indicadores de desempenho e a proposta preliminar do Instrumento de Medição de Resultados, definindo critérios objetivos para acompanhamento da execução, níveis de serviço mínimos, métricas de consumo e parâmetros de segurança.

De forma complementar, deverá ser desenvolvido um planejamento macro de transição e migração, abrangendo a estratégia de movimentação das cargas de trabalho, a preparação dos ambientes, a validação de integrações, a identificação de impactos operacionais e a definição das responsabilidades técnicas. Esse planejamento deverá considerar ainda a análise das interdependências com outras contratações, sistemas correlatos e iniciativas em curso, a fim de evitar sobreposição de escopos e assegurar a adequada coordenação técnica.

Por fim, deverá ser definida a estrutura de governança da contratação, incluindo os papéis e responsabilidades dos gestores e fiscais, os mecanismos de comunicação com a contratada, os procedimentos de homologação, aceite e monitoramento contínuo, bem como os ritos de reporte técnico e administrativo. Essas providências, tomadas em conjunto, permitirão que a instrução prossiga de forma estruturada, transparente, tecnicamente fundamentada e em conformidade com os marcos normativos aplicáveis, garantindo solidez à fase subsequente de formalização do Termo de Referência e às etapas posteriores do processo de contratação.

18. Justificativa para o Parcelamento ou não

O objeto da contratação é a prestação de Serviços de Desenvolvimento de Sistemas Críticos (Prova Prática, RST, PEV, Detran Pay), que exige a utilização de uma Solução Gerenciada de Computação em Nuvem Pública Multicloud. O não parcelamento desta contratação se justifica sob dois aspectos essenciais, que garantem a vantajosidade, segurança e eficiência para a Administração: (A) a indivisibilidade técnico-econômica da Solução Gerenciada de Nuvem e (B) a conveniência técnica e fática da aglutinação dos quatro produtos no mesmo contrato.

1. Justificativa para o Não Parcelamento da Solução Tecnológica (Desenvolvimento + Nuvem Gerenciada)

A análise técnica demonstra que o não parcelamento desta solução em contratos separados (desenvolvimento em um, hospedagem/gerenciamento em outro, ou separação de serviços de governança) é a opção mais vantajosa, segura e eficiente, fundamentada nos seguintes critérios:

18.1. Inviabilidade Técnica e Comprometimento do Desenvolvimento de Software

O parcelamento da solução resultaria em prejuízo técnico, comprometendo a engenharia de software e a continuidade institucional.

- **Necessidade de Ambiente Cloud-Native Integrado:** O desenvolvimento das funcionalidades críticas (IA Generativa, Georreferenciamento Avançado, Offline-First, Microsserviços Serverless) é impossível ou inviável no ambiente legado on-premises. O sucesso do desenvolvimento depende de um ambiente de nuvem que seja gerenciado e unificado desde o início do ciclo (DevSecOps).
- **Quebra da Governança Unificada (Cloud Brokerage):** A solução exige uma camada de Cloud Brokerage responsável por gerir simultaneamente AWS, Azure e GCP, padronizar políticas de segurança, centralizar logs e controlar custos (FinOps). O parcelamento inviabilizaria essa governança unificada, essencial para a operação segura e eficiente de ambientes de desenvolvimento e produção heterogêneos.
- **Dificuldade Crítica de Integração com Legados:** A solução de desenvolvimento necessita de integração nativa e baixa latência com os sistemas legados e corporativos do DETRAN-SP. O conhecimento arquitetural e a capacidade de integração são diferenciais estratégicos fornecidos pela solução da PRODESP, que seriam fragilizados por um parcelamento da gestão da nuvem.

18.2. Prejuízo à Economicidade e Perda de Vantajosidade (TCO)

O parcelamento da contratação resultaria em custos totais mais altos (TCO), contrariando o princípio da economicidade.

- **Perda da Economia de Escala:** A consolidação de todo o desenvolvimento e sustentação sob uma única arquitetura gerenciada gera ganhos de escala na aquisição de recursos e redução de custos administrativos e contratuais. O parcelamento levaria à contratação de serviços duplicados e ambientes paralelos, aumentando a despesa global.
- **Aumento de Custos Indiretos (Gestão):** A solução gerenciada proporciona o menor TCO ao absorver os custos de gestão, segurança (SecOps), otimização (FinOps) e governança. O parcelamento forçaria o DETRAN-SP a gerenciar múltiplos contratos, incorrendo em altos custos internos e de fiscalização.
- **Risco de Lock-in Tecnológico:** O parcelamento aumentaria o risco de amarrações a componentes proprietários específicos de um único Hyperscaler, especialmente em serviços avançados (IA/ML, geolocalização). A gestão unificada e não parcelada é fundamental para mitigar esse risco, permitindo a portabilidade e evolução arquitetural dos sistemas.

18.3. Risco Institucional e Continuidade da Sustentação

O não parcelamento é crucial para garantir a segurança jurídica e a continuidade operacional dos sistemas após o desenvolvimento.

- **Continuidade Institucional (Sustentação Futura):** O ciclo de vida planejado exige que, após o desenvolvimento, a sustentação dos novos sistemas seja transferida para o contrato de TI que o DETRAN-SP já mantém com a PRODESP. O parcelamento do desenvolvimento e/ou do gerenciamento da nuvem inviabilizaria essa transição de sustentação sem rupturas.
- **Fiscalização e Gestão Contratual:** A solução integrada simplifica a gestão e fiscalização. O parcelamento resultaria em múltiplas fiscalizações, auditorias técnicas e validações contínuas extremamente complexas, exigindo maior esforço administrativo e aumentando os riscos de passivos.
- **Segurança e Resiliência Operacional:** A Alta Disponibilidade (DR) e a resiliência são alcançadas pela distribuição e replicação de cargas de trabalho entre múltiplos ambientes e provedores. O fracionamento dessa gestão aumentaria o risco de falhas operacionais e de segurança, sendo incompatível com a criticidade dos serviços essenciais.

2. Justificativa para a Aglutinação dos Quatro Produtos na Mesma Execução Contratual

O objeto pretendido compreende o desenvolvimento de quatro sistemas estruturantes que, embora funcionalmente independentes, devem ser aglutinados na mesma execução contratual, expondo-se os motivos técnicos e fáticos pelos quais se entendeu conveniente e adequado o desenvolvimento simultâneo destes sistemas para o atendimento do interesse público, conforme detalhado a seguir:

18.4. Racionalidade Arquitetural e Tecnológica Compartilhada

O desenvolvimento dos quatro sistemas exige a adoção da mesma Arquitetura de Referência (Cloud-Native/Microserviços) e o uso dos mesmos serviços tecnológicos avançados, o que torna a aglutinação técnica e economicamente vantajosa.

- **Padrões de Integração Unificados:** Todos os sistemas exigem a criação de uma camada de API Gateway unificada e a aderência a padrões de segurança e comunicação (e.g., OAuth 2.0, OpenID Connect). O desenvolvimento aglutinado permite que esta camada seja construída e validada uma única vez, sendo reusada por todos os projetos, evitando a duplicação de esforços e a heterogeneidade técnica.
- **Reuso de Componentes de Alta Criticidade:** Componentes de infraestrutura e serviços comuns, como Plataforma de Identidade (IDP), serviços de Criptografia, Logs Centralizados e Monitoramento (Observability), são construídos para serem utilizados por todas as plataformas. O desenvolvimento simultâneo em um único contrato garante o reuso de código (code reuse), reduzindo o tempo de desenvolvimento total (Time-to-Market) e os custos operacionais (TCO).

18.5. Eficiência Operacional e Gestão de Conhecimento

A contratação única otimiza a alocação de recursos especializados e a gestão do conhecimento institucional do DETRAN-SP.

- **Otimização da Curva de Aprendizado (Onboarding):** A aglutinação permite que a equipe contratada, ao internalizar o conhecimento sobre a arquitetura e os sistemas legados do DETRAN-SP em um único processo de onboarding, aplique esse conhecimento simultaneamente nos quatro projetos. O parcelamento resultaria em quatro curvas de aprendizado independentes e custos de start-up duplicados/quadruplicados.

- **Gestão de Stakeholders Centralizada:** Os quatro sistemas possuem interdependências lógicas com os mesmos sistemas legados e envolvem os mesmos stakeholders internos (Diretorias de Habilitação, Veículos, Financeira e de TI). Uma contratação centralizada simplifica a gestão da interface e dos requisitos, evitando conflitos de prioridade, duplicação de reuniões e inconsistências na comunicação com a Administração Pública.

18.6. Vantagem Competitiva e Economicidade na Escala

A aglutinação consolida um volume de serviços complexos que atrai empresas com maior capacidade técnica e resulta em melhor proposta de valor.

- **Economia de Escala na Execução:** O desenvolvimento simultâneo de quatro grandes plataformas permite ao contratado otimizar a alocação de recursos (e.g., analistas de requisitos, arquitetos de segurança e DevOps), aplicando os mesmos profissionais especialistas em fases não concorrentes dos diferentes projetos. Este ganho de escala se reverte em menor custo unitário por sistema para a Administração.
- **Atração de Soluções Abrangentes:** O objeto de grande porte e de alta complexidade atrai fornecedores com estrutura e expertise comprovadas em grandes projetos de Governo Digital, garantindo maior competitividade e qualidade técnica superior na execução, o que é fundamental para a criticidade dos sistemas.

Conclusão

Diante do exposto, o desenvolvimento de sistemas usando uma solução de Serviços Gerenciados de Nuvem Pública Multicloud, com a aglutinação dos quatro sistemas críticos, constitui uma unidade técnica e funcional indivisível para atender, de forma segura, contínua e econômica, às necessidades institucionais do DETRAN-SP. O parcelamento da solução acarreta prejuízo à economicidade, compromete a segurança e governança e eleva a complexidade de gestão e fiscalização.

Portanto, a contratação deverá ocorrer de forma não parcelada para garantir a integralidade da solução, a continuidade dos serviços essenciais e o atendimento pleno aos requisitos estabelecidos neste ETP.

19. Contratações Correlatas/Interdependentes

A presente contratação é correlata e interdependente do Contrato vigente nº 097/2025, que tem por objeto a hospedagem e nuvem pública (multiclouds), sendo também o contrato, ou eventual substituto que dê continuidade a ele, utilizado para a manutenção e sustentação dos sistemas desenvolvidos na contratação atual.

Durante a fase de desenvolvimento e vigência do contrato de 12 meses, a sustentação dos sistemas legados e operacionais atuais seguirá no contrato nº 003/2024 de serviços de TI atualmente vigente com a PRODESP. Após a implantação final dos novos sistemas desenvolvidos, a sustentação da nova arquitetura Cloud-Native será migrada e absorvida pelo contrato de Multiclouds que estiver vigente com a PRODESP, garantindo a continuidade operacional e a racionalidade financeira do ciclo de vida dos sistemas.

20. Alinhamento contratação e Plano anual

O objeto da contratação está previsto no Plano de Contratações Anual 2026, nos termos do Decreto Estadual nº 67.689, de 3 de maio de 2023, conforme detalhamento a seguir:

1. ID PCA no PNCP: 15519361000116-0-000004/2026;
2. Data de publicação no PNCP: 30/06/2025;
3. Id do item no PCA: 50;
4. Classe/Grupo: SERVIÇOS DE PESQUISA, ANÁLISE E DESENVOLVIMENTO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC);
5. Identificador da Futura Contratação: 532403-55/2026.

21. Possíveis Impactos Ambientais

As informações relativas aos possíveis impactos ambientais e sustentabilidade, foram dispostas ao longo desse Estudo Técnico Preliminar, sendo abordadas nos seguintes itens:

- 10.2 - Hospedagem On-Premises / Expansão de Datacenter Próprio: onde a inviabilidade da infraestrutura local é justificada por implicar custos desproporcionalmente elevados em refrigeração e energia, o que evidencia os maiores impactos ambientais dessa alternativa; e
- 15.1 - Justificativa Econômica: onde se demonstra que a solução em nuvem elimina a necessidade de investimentos em refrigeração, energia e manutenção predial, bem como a aquisição e descarte de hardware, configurando uma vantagem econômica e ambiental.

22. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

22.1. Justificativa da Viabilidade

Com base nas informações levantadas neste Estudo Técnico Preliminar, nas análises de necessidade, nos requisitos de negócio e tecnológicos identificados, na estimativa de demanda, na avaliação comparativa de soluções disponíveis no mercado e na análise preliminar de custos, conclui-se que há viabilidade técnica, operacional e econômica para o prosseguimento da instrução, visando à elaboração do Termo de Referência e demais etapas necessárias à eventual contratação da solução de Serviços de Desenvolvimento de Sistemas em Nuvem. A presente declaração decorre da compatibilidade entre as necessidades institucionais do DETRAN-SP e as capacidades oferecidas pela solução analisada, da aderência às diretrizes de transformação digital do Estado e das evidências preliminares de que a adoção de arquitetura em nuvem tem potencial para atender de forma adequada às exigências de continuidade, segurança, escalabilidade, governança e eficiência financeira relacionadas aos sistemas finalísticos e corporativos do órgão. Ressalta-se que esta declaração possui caráter meramente indicativo e preliminar, estando restrita à fase de estudos, não configurando decisão de contratação, escolha definitiva da solução ou autorização de despesas. Sua finalidade é apenas atestar que, no contexto das análises realizadas até esta etapa, existe fundamentação suficiente para permitir que o processo avance para a elaboração do Termo de Referência, a avaliação jurídica, a adequação orçamentária e as demais fases previstas na legislação. O prosseguimento do processo permanece condicionado às manifestações técnicas, jurídicas e orçamentárias que serão emitidas nas etapas subsequentes, bem como às aprovações previstas nos normativos internos e nos mecanismos de governança do Estado de São Paulo.

23. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

BRUNO ZAIA BONETO

Diretor de Tecnologia da Informação



Assinou eletronicamente em 02/02/2026 às 09:30:52.