



SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
DIVISÃO DE GESTÃO DE FROTAS - DIFRO/CGAD/DLOG/PF

ANEXO I

REQUISITOS TÉCNICOS DO SISTEMA - WEB SERVICE/ API

1. SERVIÇO DE WEB SERVICE/ API

1.1. Este ANEXO tem por objeto estabelecer os requisitos técnicos que deverão ser atendidos pelos sistemas de ABASTECIMENTO e MANUTENÇÃO da Frota da Polícia Federal, com vistas a garantir a correta disponibilização, operação e manutenção do serviço de Web Service/API. A solução deverá assegurar integração segura, contínua, padronizada e escalável, observando os princípios da interoperabilidade (art. 12, Lei 14.133/2021), governança digital, proteção de dados pessoais (Lei 13.709/2018 – LGPD) e segurança da informação.

1.1.1. A integração deverá ser documentada, testada em ambiente de homologação (sandbox) e validada pela equipe técnica da CONTRATANTE antes da entrada em produção. A integração deverá contemplar, no mínimo, as seguintes informações:

- a) Serviços de manutenção realizados nos veículos e embarcações da CONTRATANTE;
- b) Registros de abastecimento;
- c) Dados cadastrais e operacionais dos condutores;
- d) Informações técnico-administrativas dos veículos e embarcações da CONTRATANTE;
- e) Indicadores de depreciação veicular, com base na Tabela FIPE.

1.2. **Interoperabilidade entre Sistemas:** O sistema da CONTRATADA deverá garantir plena interoperabilidade entre sistemas, mediante o fornecimento de interfaces de programação de aplicações (APIs) padronizadas, que permitam o consumo automatizado de dados. As APIs deverão assegurar a integridade, rastreabilidade e disponibilidade das informações, conforme os requisitos técnicos e operacionais definidos no contrato e em seus anexos.

1.3. **Requisitos Funcionais da Web Service/API:** A Web Service/API a ser disponibilizada pela CONTRATADA deverá atender aos seguintes requisitos técnicos e operacionais:

- a) Permitir o fornecimento automatizado e tempestivo de dados estruturados relacionados à manutenção, abastecimento, condutores, veículos e embarcações, conforme especificado no item 3.4 deste ANEXO;
- b) Viabilizar consultas individualizadas, preferencialmente por número de placa, utilizando protocolos e formatos amplamente aceitos, como HTTPS, JSON e XML;
- c) Disponibilizar os dados em formato estruturado, compatível com ferramentas de Business Intelligence (BI), permitindo sua integração em painéis e relatórios gerenciais;
- d) Assegurar compatibilidade, preferencialmente, com as tecnologias de BI já adotadas pela CONTRATANTE, como Microsoft Power BI e Qlik Sense, favorecendo a continuidade tecnológica e o aproveitamento da infraestrutura existente;
- e) Atender integralmente aos requisitos de segurança da informação, desempenho, escalabilidade, suporte técnico e alta disponibilidade, conforme especificações constantes deste ANEXO e demais documentos contratuais.

2. ACESSO E SEGURANÇA

2.1. **Disponibilização de Interface e Controle de Acesso:** A CONTRATADA deverá disponibilizar serviço de Web Service/API com controle de acesso baseado em OAuth 2.0 ou protocolo equivalente de mercado, com API Tokens criptograficamente seguros, exclusivos e intransferíveis, associados a perfis de acesso. Deverão existir camadas adicionais de segurança, incluindo MFA (autenticação multifator) para administradores, registro de logs imutáveis e alertas automáticos de uso suspeito. O sistema deverá permitir gestão centralizada dos tokens, com painel de controle para a CONTRATANTE acompanhar acessos, revogações e histórico de uso.

2.2. **Requisitos Técnicos e Operacionais do API Token:** O API Token fornecido pela CONTRATADA deverá atender aos seguintes requisitos:

- a) Ser gerado de forma criptograficamente segura, exclusivo por cliente e intransferível;
- b) Possuir validade configurável e renovação periódica, conforme boas práticas de segurança da informação;
- c) Ter seu ciclo de vida (emissão, renovação e revogação) integralmente gerenciado pela CONTRATADA, com documentação técnica clara e atualizada;
- d) Incluir mecanismo de aviso prévio à CONTRATANTE, com antecedência mínima de 72 (setenta e duas) horas, em caso de expiração programada ou necessidade de revogação;
- e) Ser validado a cada requisição, permitindo apenas o processamento de solicitações autenticadas. Requisições com token inválido ou expirado deverão ser recusadas automaticamente, com retorno padronizado de erro.

2.3. A comunicação entre os sistemas da CONTRATANTE e o serviço de Web Service/API disponibilizado pela CONTRATADA deverá ocorrer exclusivamente por meio do protocolo HTTPS (Hypertext Transfer Protocol Secure), com utilização obrigatória da versão 1.2 ou superior do padrão TLS (Transport Layer Security). Esse protocolo deverá assegurar:

- a) Confidencialidade, mediante proteção contra interceptações durante o tráfego de dados;
- b) Integridade, por meio da prevenção de alterações indevidas nas informações transmitidas;
- c) Autenticidade, garantindo que a comunicação ocorra exclusivamente com o servidor legítimo da CONTRATADA.

2.4. A CONTRATADA será integralmente responsável pela adoção e manutenção de medidas de segurança da informação, devendo garantir:

- a) Proteção contra vazamento, uso indevido ou acesso não autorizado aos tokens de autenticação;
- b) Monitoramento contínuo e registro de logs de acesso, com finalidade de auditoria e rastreabilidade;
- c) Implementação de mecanismos de defesa contra ataques cibernéticos, incluindo tentativas de repetição (replay), sobrecarga (DoS/DDoS) e intrusão;
- d) Manutenção de infraestrutura tecnológica segura e atualizada, com uso obrigatório de certificados digitais válidos, emitidos por autoridade certificadora reconhecida oficialmente.

2.5. A CONTRATADA deverá observar integralmente as disposições da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), bem como as normas técnicas e regulamentos internos da CONTRATANTE, responsabilizando-se pelo tratamento adequado, seguro e lícito de todos os dados pessoais acessados, coletados, armazenados ou processados no âmbito da execução contratual.

3. ESTRUTURA E RETORNO DE DADOS

3.1. A API deverá disponibilizar endpoints dedicados, entendidos como endereços eletrônicos específicos dentro do serviço Web Service/API, responsáveis por prover, de forma segmentada, os diferentes conjuntos de dados exigidos por esta contratação. Esses endpoints deverão ser claramente identificáveis, documentados e organizados por tipo de informação, permitindo que os sistemas da CONTRATANTE realizem consultas diretas, automatizadas e individualizadas às seguintes categorias de dados:

- a) Manutenção do veículos ou embarcações;
- b) Abastecimento dos veículos ou embarcações;
- a) Dados cadastrais e operacionais dos condutores;
- b) Informações técnicas e administrativas dos veículos ou embarcações;
- c) Dados de avaliação e depreciação veicular com base na Tabela FIPE.

3.2. As consultas à Web Service/API deverão ser orientadas, prioritariamente, pelo número da placa dos veículos ou embarcações, admitindo-se também outros parâmetros de pesquisa, como período, identificador do condutor, entre outros, conforme documentação técnica fornecida pela CONTRATADA.

3.3. Os dados deverão ser disponibilizados em **formatos abertos e não proprietários (JSON, XML, CSV)**, compatíveis com processos de ETL, garantindo interoperabilidade com sistemas públicos. Cada endpoint deverá trazer campos obrigatórios padronizados e validados em conformidade com o Vocabulário Comum de Dados da Administração Pública Federal (Vocab-APF), permitindo integração eficiente com ferramentas de análise e Business Intelligence (BI).

3.4. Os dados retornados pela API deverão conter, no mínimo, os campos obrigatórios especificados para cada tipo de **endpoint**, conforme descrito a seguir:

3.4.1. Para o endpoint de **manutenção de veículos ou embarcações**, os dados deverão incluir:

- a) Identificador único da manutenção;
- b) Placa do veículo ou embarcação;
- c) Tipo do serviço executado;
- d) Data de execução;
- e) Valor do serviço;
- f) Nome do fornecedor;
- g) Observações técnicas ou operacionais.

3.4.2. Para o endpoint de **abastecimento**, os dados deverão incluir:

- a) Identificador do abastecimento;
- b) Data da operação;
- c) Valor abastecido;
- d) Local de abastecimento;
- e) Quilometragem registrada;
- f) Identificação do condutor;
- g) Placa do veículo ou embarcação.

3.4.3. Para o endpoint de **condutor**, os dados deverão incluir:

- a) Identificador do condutor;
- b) Nome completo;
- c) CPF;
- d) Registro ou matrícula funcional;
- e) Número e categoria da CNH;
- f) Data de validade da CNH;
- g) Status (ativo/inativo);

- h) Cargo ou função;
- i) Tipo de vínculo;
- j) Telefone de contato.

3.4.4. Para o endpoint de **veículos ou embarcações**, os dados deverão incluir:

- a) Identificador do veículo ou embarcação;
- b) Placa;
- c) Marca;
- d) Modelo;
- e) Tipo de combustível;
- f) Quilometragem atual;
- g) Capacidade do tanque;
- h) Saldo de abastecimento disponível;
- i) Saldo total contratado.

3.4.1. Para o endpoint de **depreciação veicular**, os dados deverão incluir:

- a) Marca, modelo e ano do veículo;
- b) Valor de mercado atualizado (Tabela FIPE);
- c) Data da última atualização do valor;
- d) Percentual estimado de depreciação acumulada (quando aplicável);
- e) Fonte oficial da informação utilizada.

3.5. A CONTRATADA deverá realizar a validação prévia de todos os dados disponibilizados pela API, assegurando que estejam consistentes, completos, livres de campos nulos indevidos e em conformidade com o dicionário de dados fornecido pela CONTRATANTE. Essa validação é essencial para garantir a integridade das informações trafegadas entre os sistemas e a confiabilidade dos processos de gerenciamento de frota.

3.6. A API deverá adotar versionamento explícito nos endpoints (ex.: /v1/, /v2/), com documentação técnica comparativa entre versões, changelog acessível e ambiente de testes (sandbox) para validação prévia. Toda nova versão deverá manter compatibilidade retroativa por no mínimo 6 meses, salvo em casos críticos de segurança.

3.7. Qualquer alteração na estrutura dos dados disponibilizados pela API, incluindo a inclusão, modificação ou remoção de campos, deverá observar os seguintes requisitos:

- a) comunicação formal à CONTRATANTE com antecedência mínima de 10 (dez) dias úteis, informando detalhadamente as mudanças propostas;
- b) disponibilização de ambiente de testes (sandbox) para validação da nova estrutura por parte da CONTRATANTE; e
- c) atualização integral da documentação técnica, incluindo o dicionário de dados, refletindo todas as alterações realizadas.

4. PERFORMANCE E DISPONIBILIDADE

4.1. O serviço de Web Service/API deverá operar em regime de alta disponibilidade, com funcionamento contínuo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

4.2. A CONTRATADA deverá garantir índice mínimo de disponibilidade mensal de **99,5%**, com monitoramento contínuo por ferramenta externa independente, relatórios de SLA mensais e penalidades automáticas em caso de descumprimento. O tempo médio de resposta (latência) não poderá ultrapassar **2 segundos** em 95% das requisições. Em caso de descumprimento, deverão ser aplicadas penalidades contratuais progressivas, conforme impacto operacional, com possibilidade de substituição da solução em caso de reincidência.

4.3. O tempo de resposta das requisições à API deverá ser compatível com aplicações em tempo real, assegurando desempenho adequado para os processos de gerenciamento de frota.

4.4. A CONTRATADA deverá manter monitoramento ativo e contínuo do serviço, observando os seguintes requisitos:

- a) geração de relatórios periódicos contendo indicadores de disponibilidade, performance e falhas detectadas;
- b) disponibilização dos relatórios à CONTRATANTE mediante solicitação formal;
- c) implementação de sistema de monitoramento em tempo real, com alertas automáticos em caso de falhas, lentidão ou indisponibilidade.

4.5. Antes da homologação da solução, a CONTRATADA deverá realizar testes de carga e stress, apresentando relatório técnico que comprove a escalabilidade e a estabilidade da API sob diferentes condições de uso.

4.6. **Monitoramento Inteligente com IA:** A CONTRATADA deverá implementar mecanismos de monitoramento inteligente baseados em inteligência artificial e machine learning, capazes de identificar padrões anômalos, prever indisponibilidades e bloquear automaticamente acessos suspeitos. Os alertas deverão ser enviados em tempo real à CONTRATANTE e armazenados em log seguro para auditoria.

5. INTEGRAÇÃO COM SOLUÇÕES DE BUSINESS INTELLIGENCE (BI)

5.1. A estrutura dos dados fornecidos pela API deverá ser compatível com soluções de Business Intelligence (BI), de modo a permitir sua ingestão, transformação e análise por ferramentas analíticas utilizadas pela CONTRATANTE, observando os seguintes requisitos:

- 5.1.1. Os dados deverão ser organizados e padronizados de forma a viabilizar visualizações por meio de painéis gerenciais e analíticos, com foco na tomada de decisões estratégicas e operacionais;
- 5.1.2. A estrutura dos dados deverá ser nativamente compatível com ferramentas de BI utilizadas pela CONTRATANTE, como Microsoft Power BI e Qlik Sense, incluindo conectores diretos, documentação de integração e suporte técnico para configuração de painéis analíticos.
- 5.1.3. A estrutura dos dados deverá permitir a automação de processos de extração e atualização periódica das informações, respeitando os padrões técnicos definidos pela CONTRATANTE.

6. DOCUMENTAÇÃO TÉCNICA

6.1. A CONTRATADA deverá fornecer documentação técnica em português, em portal eletrônico com acesso autenticado, no formato *Swagger/OpenAPI*, permitindo testes em tempo real (sandbox). Toda atualização deverá vir acompanhada de changelog e histórico de versões, contendo, no mínimo, as seguintes informações:

- a) instruções detalhadas sobre o processo de autenticação e utilização do API Token, incluindo fluxos e exemplos práticos;
- b) descrição dos endpoints disponíveis, com especificação dos parâmetros obrigatórios e opcionais, bem como os métodos HTTP utilizados;
- c) exemplos de chamadas de requisição e respectivas respostas esperadas, nos formatos JSON e XML, contemplando diferentes cenários de uso;
- d) tabela de códigos de erro e mensagens associadas, acompanhadas de orientações para tratamento adequado por parte da CONTRATANTE;
- e) políticas de controle de acesso, diretrizes de segurança e boas práticas recomendadas para integração e consumo da API.

6.2. Sempre que houver atualização na API, a CONTRATADA deverá revisar e disponibilizar à

CONTRATANTE a documentação técnica correspondente, observando os seguintes requisitos:

- a) a documentação atualizada deverá ser entregue com antecedência mínima de 5 (cinco) dias úteis antes da entrada em vigor das alterações;
- b) o conteúdo revisado deverá refletir integralmente as modificações realizadas, incluindo ajustes nos endpoints, parâmetros, formatos de resposta e códigos de erro;
- c) a disponibilização deverá ocorrer em meio digital, em língua portuguesa, garantindo fácil acesso e compreensão por parte da equipe técnica da CONTRATANTE.

7. SUPORTE TÉCNICO

7.1. A CONTRATADA deverá garantir suporte técnico durante toda a vigência do contrato, assegurando atendimento tempestivo para esclarecimento de dúvidas, resolução de falhas técnicas e auxílio na integração da API com os sistemas da CONTRATANTE, de forma contínua e eficaz, por meio de equipe qualificada e canais de comunicação previamente definidos entre as partes.

7.2. O suporte técnico deverá estar disponível durante toda a vigência do contrato, por meio de canais dedicados, como e-mail institucional e telefone, observando os seguintes prazos máximos de resposta, conforme o nível de criticidade da ocorrência:

- a) até 4 (quatro) horas úteis para erros que impeçam a operação do serviço;
- b) até 1 (um) dia útil para erros com impacto parcial no funcionamento da API;
- c) até 2 (dois) dias úteis para dúvidas técnicas e operacionais relacionadas à integração ou ao uso da solução.

7.3. A CONTRATADA deverá manter registro formal e sistemático de todos os atendimentos realizados no âmbito do suporte técnico, contendo o controle dos prazos de resposta e resolução, a descrição da solução adotada e a identificação dos responsáveis pelo atendimento, garantindo rastreabilidade e transparência no relacionamento com a CONTRATANTE.

7.4. A CONTRATADA deverá disponibilizar, no mínimo, **160 (cento e sessenta) horas técnicas de consultoria especializada**, a serem utilizadas durante a vigência do contrato, sem custo adicional à CONTRATANTE. As horas deverão ser prestadas sob demanda, em dias e horários previamente acordados, podendo incluir:

- a) Apoio na implementação da API e integração com os sistemas da CONTRATANTE;
- b) Suporte técnico na estruturação de painéis e dashboards em ferramentas de Business Intelligence (BI), como Microsoft Power BI e Qlik Sense;
- c) Orientações para uso adequado dos dados retornados pela API, definição de indicadores e boas práticas analíticas;
- d) Esclarecimento de dúvidas técnicas e operacionais relacionadas à solução contratada.

7.4.1. A CONTRATANTE poderá solicitar a substituição de consultores ou a redistribuição das horas conforme a evolução das demandas técnicas, sendo obrigatório o registro formal das atividades realizadas, com controle de saldo, escopo e resultados entregues.

8. BACKUP E RECUPERAÇÃO DE DADOS

8.1. A CONTRATADA deverá implementar política de backup diário incremental e semanal completo, com retenção mínima de 5 anos. Os backups deverão ser armazenados em ambiente segregado e testados periodicamente por meio de simulações de recuperação de desastre (DRP – Disaster Recovery Plan).

8.2. Os procedimentos de backup deverão ser devidamente documentados e auditáveis, contemplando mecanismos que permitam a restauração segura e eficiente dos dados, sempre que necessário, conforme os padrões técnicos estabelecidos pela CONTRATANTE.

9. CONTROLE DE LIMITES E ESCALABILIDADE

9.1. A API deverá ser capaz de suportar elevado volume de requisições simultâneas, inclusive durante períodos de alta demanda, garantindo estabilidade, desempenho e continuidade dos serviços prestados à CONTRATANTE.

9.2. A CONTRATADA deverá implementar mecanismo de controle de taxa de requisições (rate limiting), com configuração flexível e ajustável, visando prevenir abusos, proteger a infraestrutura e assegurar o funcionamento adequado da API em diferentes cenários de uso.

9.3. O limite de requisições simultâneas, por minuto ou por hora, deverá ser previamente acordado com a CONTRATANTE com base em estudo técnico do volume esperado, podendo ser revisado ao longo da execução contratual conforme o crescimento da demanda e a evolução dos sistemas integrados.

10. ATUALIZAÇÕES E EVOLUÇÕES

10.1. A CONTRATADA deverá manter a API continuamente atualizada, com foco na:

- a) correção de erros identificados durante o uso ou nos processos de integração;
- b) inclusão de melhorias tecnológicas e aprimoramentos relacionados à segurança da informação;
- c) atendimento a novas demandas funcionais apresentadas pela CONTRATANTE, visando à evolução da solução conforme necessidades operacionais.

10.2. Correções críticas deverão ser implementadas em até **24 horas**, com comunicação imediata à CONTRATANTE. Alterações não críticas deverão ser liberadas em ciclos trimestrais de atualização planejada, com publicação de roadmap tecnológico.

10.3. Toda atualização da API deverá ser precedida de comunicação formal à CONTRATANTE, contendo informações técnicas detalhadas sobre os impactos previstos, os prazos de execução e os procedimentos de transição, de modo a assegurar o planejamento adequado e a adaptação dos sistemas integrados.

11. DISPOSIÇÕES FINAIS

11.1. A CONTRATADA será integralmente responsável pela disponibilização, operação, segurança, atualização e manutenção contínua do serviço de Web Service/API, incluindo a infraestrutura técnica necessária para sua hospedagem e funcionamento estável, sem prejuízo à continuidade dos serviços.

11.2. Todas as obrigações técnicas descritas neste ANEXO deverão ser rigorosamente observadas e implementadas pela CONTRATADA durante toda a vigência do contrato, sendo vedada qualquer interrupção ou degradação do serviço, salvo nos casos previamente autorizados e acordados com a CONTRATANTE.

11.3. Toda e qualquer alteração na estrutura da API, nos dados disponibilizados, nos mecanismos de autenticação ou nos parâmetros de segurança deverá ser formalmente comunicada à CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis, acompanhada da respectiva atualização da documentação técnica.

11.4. A CONTRATADA deverá garantir que os dados fornecidos estejam sempre atualizados, íntegros e consistentes, mantendo sua responsabilidade sobre a origem, precisão e completude das informações disponibilizadas por meio da API.

11.5. É de responsabilidade exclusiva da CONTRATADA o cumprimento das normas legais aplicáveis à proteção de dados, segurança da informação e disponibilidade dos serviços, observando as diretrizes estabelecidas pela Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), bem como as normas técnicas e regulamentos internos da CONTRATANTE, quando aplicáveis.

11.6. As funcionalidades da API e os dados fornecidos deverão atender às necessidades

operacionais, administrativas e estratégicas da CONTRATANTE, permitindo integração fluida com seus sistemas internos e extração eficiente de informações para fins de controle, auditoria e tomada de decisão.

11.7. A CONTRATADA deverá manter comunicação direta com as áreas técnicas da CONTRATANTE, por meio de canal oficial previamente indicado, para esclarecimentos técnicos, resolução de problemas e alinhamentos operacionais, sempre que solicitado.

11.8. Quaisquer omissões ou lacunas técnicas não previstas neste documento, mas que se revelem indispensáveis para o cumprimento pleno do objeto contratual, deverão ser supridas pela CONTRATADA sem ônus adicional à Administração, desde que estejam diretamente vinculadas à operacionalização do serviço descrito.

11.9. As horas de consultoria técnica previstas neste ANEXO deverão ser disponibilizadas sem custo adicional à CONTRATANTE, estando compreendidas no escopo da prestação continuada dos serviços contratados. A CONTRATANTE poderá solicitar a substituição de consultores ou a redistribuição das horas conforme a evolução das demandas técnicas, desde que mantido o saldo contratado.



Documento assinado eletronicamente por **ANDRE LUIZ BARBOSA RODRIGUES, Perito(a) Criminal Federal**, em 06/02/2026, às 14:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **WILLIAM ENIO GUEDES FABRICIO, Chefe de Divisão**, em 06/02/2026, às 14:41, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei4.pf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=144608008&crc=50E65DFA.
Código verificador: **144608008** e Código CRC: **50E65DFA**.