



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

ANEXO K

REQUISITOS TÉCNICOS PARA CONTRATAÇÃO DE SERVIÇO DE WEB SERVICE/ API

1. SERVIÇO DE WEB SERVICE/ API

1.1. O presente Anexo tem por objeto a contratação de empresa especializada na disponibilização, operação e manutenção de serviço de Web Service/ API, com a finalidade de estabelecer integração segura, contínua e estruturada entre os sistemas internos da Polícia Federal e as bases de dados da empresa contratada, contendo informações relativas a:

- Serviços de manutenção realizados nas viaturas;
- Abastecimentos registrados;
- Dados cadastrais e operacionais dos condutores;
- Informações técnico-administrativas das viaturas oficiais;
- Indicadores de depreciação veicular, com base em sistemas reconhecidos no mercado, como a Tabela FIPE

1.2. A solução a ser contratada deverá assegurar a interoperabilidade entre sistemas, viabilizando o consumo automatizado e padronizado de dados por meio de interfaces de programação de aplicações (APIs), de forma a garantir a integridade, rastreabilidade e disponibilidade das informações.

1.3. A Web Service/API deverá ser concebida para :

- a) Disponibilizar, de forma automatizada e tempestiva, dados estruturados sobre manutenção, abastecimento, condutores e viaturas, conforme detalhado no item 3.4.
- b) Possibilitar consultas individualizadas, preferencialmente por número de placa das viaturas, utilizando protocolos e formatos amplamente aceitos, como HTTPS, JSON e XML;
- c) Disponibilizar os dados de forma estruturada, compatível com processos de extração e análise por soluções de Business Intelligence (BI), permitindo sua utilização em painéis e relatórios gerenciais, conforme os padrões de ferramentas como Microsoft Power BI e Qlik Sense;
- d) Assegurar, preferencialmente, a compatibilidade com tecnologias de BI já utilizadas pela Polícia Federal, tais como Microsoft Power BI e Qlik Sense, favorecendo a continuidade tecnológica, o reaproveitamento de infraestrutura e a eficiência na análise de dados;
- e) Atender plenamente aos requisitos de segurança da informação, desempenho, escalabilidade, suporte técnico e alta disponibilidade, conforme especificado nos demais itens deste Anexo.

1.4. A contratada será responsável pela infraestrutura necessária para hospedagem, gestão e operação da API, bem como pela disponibilização de documentação técnica, suporte técnico especializado e mecanismos de controle de acesso, garantindo a plena integração com os sistemas da Polícia Federal durante toda a vigência contratual.

2. ACESSO E SEGURANÇA

2.1. A contratada deverá disponibilizar o serviço de Web Service/ API com mecanismo de

controle de acesso baseado em API Token, o qual é um código de autenticação digital exclusivo, utilizado para validar e autorizar o acesso da Polícia Federal aos dados protegidos da interface

2.2. O API Token deverá atender aos seguintes requisitos técnicos e operacionais:

- a) Ser gerado de forma criptograficamente segura, exclusivo por cliente e intransferível;
- b) Possuir validade configurável e ser renovável periodicamente, conforme boas práticas de segurança da informação;
- c) Ter seu ciclo de vida (emissão, renovação, revogação) integralmente gerenciado pela contratada, a qual deverá fornecer documentação técnica clara e atualizada;
- d) Prever mecanismo de aviso prévio à contratante, com no mínimo 72 (setenta e duas) horas de antecedência, sempre que houver expiração programada ou necessidade de revogação;
- e) Ser validado a cada requisição, garantindo que apenas solicitações autenticadas sejam processadas. Requisições sem token válido ou com token expirado deverão ser automaticamente recusadas, com retorno padronizado de erro.

2.3. A comunicação entre os sistemas da Polícia Federal e o serviço de Web Service/API deverá ocorrer exclusivamente via protocolo HTTPS (Hypertext Transfer Protocol Secure), utilizando TLS (Transport Layer Security) versão 1.2 ou superior, que assegure:

- Confidencialidade: proteção contra interceptações durante o tráfego de dados;
- Integridade: prevenção de alterações nos dados durante a transmissão;
- Autenticidade: garantia de que a comunicação está ocorrendo com o servidor legítimo da contratada.

2.4. A contratada será integralmente responsável pela aplicação de medidas de segurança da informação, incluindo:

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

2.5. A CONTRATADA deverá cumprir integralmente a Lei nº 13.709/2018 (LGPD), bem como as normas técnicas e regulamentos internos da Polícia Federal, responsabilizando-se pelo tratamento adequado e seguro de todos os dados pessoais acessados ou processados no âmbito deste contrato.

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 Polícia Federal realizem consultas diretas, automatizadas e individualizadas às seguintes categorias de dados:

- a) Manutenção das viaturas;
- b) Abastecimento das viaturas;
- a) Dados cadastrais e operacionais dos condutores;
- b) Informações técnicas e administrativas das viaturas;
- c) Dados de avaliação e depreciação veicular, com base em fontes reconhecidas como a Tabela FIPE.

3.2. As consultas deverão ser orientadas, prioritariamente por número da placa da viatura,

podendo também aceitar outros parâmetros de pesquisa (como período, identificador do condutor, entre outros), conforme documentado pela contratada.

3.3. Os dados disponibilizados deverão estar disponíveis nos formatos JSON e XML, com estrutura claramente documentada, padronizada e compatível com os processos de ingestão, transformação e carga (ETL) das ferramentas de análise e Business Intelligence (BI).

3.4. Os dados retornados deverão conter, no mínimo, os seguintes campos obrigatórios por tipo de endpoint:

3.4.1. **Manutenção da viatura:**

- Identificador único da manutenção;
- Placa da viatura;
- Tipo do serviço executado;
- Data de execução;
- Valor do serviço;
- Nome do fornecedor;
- Observações técnicas ou operacionais.

3.4.2. **Abastecimento:**

- Identificador do abastecimento;
- Data da operação;
- Valor abastecido;
- Local de abastecimento;
- Quilometragem registrada;
- Identificação do condutor;
- Placa da viatura.

3.4.3. **Condutor:**

- Identificador do condutor;
- Nome completo;
- CPF;
- Registro ou matrícula funcional;
- Número e categoria da CNH;
- Data de validade da CNH;
- Status (ativo/inativo);
- Cargo ou função;
- Tipo de vínculo;
- Telefone de contato.

3.4.4. **Viatura:**

- Identificador da viatura;
- Placa;
- Marca;
- Modelo;
- Tipo de combustível;
- Quilometragem atual;
- Capacidade do tanque;
- Saldo de abastecimento disponível;
- Saldo total contratado.

3.4.1. Depreciação veicular:

- Marca, modelo e ano do veículo;
- Valor de mercado atualizado (com base em fonte como Tabela FIPE);
- Data da última atualização do valor;
- Percentual estimado de depreciação acumulada (quando aplicável);
- Fonte oficial da informação utilizada.

3.5. A CONTRATADA deverá validar previamente todos os dados disponibilizados pela API, assegurando consistência, completude, ausência de campos nulos indevidos e conformidade com o dicionário de dados fornecido.

3.6. A API deverá adotar mecanismo de versionamento explícito, com identificador de versão (ex: /v1/, /v2/) nos endpoints, a fim de permitir a coexistência de versões e evitar interrupção de serviços existentes em caso de atualização.

3.7. Qualquer alteração na estrutura dos dados, inclusão ou remoção de campos, deverá ser precedida de:

- Comunicação formal à contratante com antecedência mínima de 10 (dez) dias úteis;
- Disponibilização de versão de testes (sandbox) para validação da nova estrutura;
- Atualização integral da documentação técnica e dicionário de dados.

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%, devendo constar cláusula contratual específica de Acordo de Nível de Serviço (SLA), com previsão de sanções administrativas em caso de descumprimento.

4.3. O tempo de resposta das requisições à API deverá ser compatível com aplicações em tempo real.

4.4. A contratada deverá manter monitoramento ativo do serviço, com geração de relatórios periódicos de disponibilidade, performance e falhas detectadas, os quais deverão ser compartilhados com a contratante mediante solicitação.

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), possibilitando sua ingestão e transformação por ferramentas analíticas utilizadas na contratante.

5.2. Os dados deverão ser organizados e padronizados de forma a permitir visualizações por meio de painéis gerenciais e analíticos, com foco na tomada de decisões estratégicas e operacionais.

5.3. Será considerada preferencial a compatibilidade com ferramentas de BI já em uso pela Polícia Federal, especialmente Microsoft Power BI e Qlik Sense, facilitando a integração com a infraestrutura já implantada.

6. DOCUMENTAÇÃO TÉCNICA

6.1. A contratada deverá fornecer documentação técnica completa, atualizada e em língua portuguesa, contendo no mínimo:

- a) Instruções detalhadas sobre o processo de autenticação e uso do API Token;
- b) Lista descritiva dos endpoints disponíveis, com seus parâmetros obrigatórios e

opcionais;

c) Exemplos de chamadas de requisição e respostas esperadas, nos formatos JSON e XML;

d) Tabela de códigos de erro e mensagens associadas, com orientações para tratamento adequado;

e) Políticas de controle de acesso, segurança e boas práticas recomendadas.

6.2. Sempre que houver atualização na API, a documentação deverá ser revista e disponibilizada à contratante com antecedência mínima de 5 (cinco) dias úteis da entrada em vigor das alterações.

7. SUPORTE TÉCNICO

7.1. A contratada deverá garantir suporte técnico durante toda a vigência do contrato, para atendimento de dúvidas, resolução de falhas e auxílio na integração com os sistemas da Polícia Federal.

7.2. O suporte técnico deverá estar disponível por meio de canais dedicados, como e-mail institucional e telefone, com tempo máximo de resposta conforme níveis de criticidade:

- Erros que impedem a operação do serviço: resposta em até 4 (quatro) horas úteis;
- Erros com impacto parcial: resposta em até 1 (um) dia útil;
- Dúvidas técnicas e operacionais: resposta em até 2 (dois) dias úteis.

7.3. A contratada deverá manter registro formal de todos os atendimentos realizados, com controle de prazos, solução adotada e responsáveis.

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, para apoio na implementação da API, integração com os sistemas internos da Polícia Federal e estruturação de painéis em ferramentas de Business Intelligence (BI). As horas deverão ser prestadas sob demanda da contratante, em dias e horários previamente acordados, podendo incluir:

- Apoio técnico à equipe da contratante na integração dos dados aos sistemas internos;
- Suporte na construção dos painéis e dashboards analíticos com Power BI ou Qlik Sense;
- Orientações para uso adequado dos dados retornados pela API e definição de indicadores.

8. BACKUP E RECUPERAÇÃO DE DADOS

8.1. A contratada deverá implementar política de backup periódico, visando à preservação e recuperação de dados operacionais relevantes utilizados no funcionamento da API.

8.2. Os procedimentos de backup deverão ser documentados e auditáveis, garantindo a restauração em caso de falha, perda ou corrupção de dados.

9. CONTROLE DE LIMITES E ESCALABILIDADE

9.1. A API deverá suportar elevado volume de requisições simultâneas, inclusive em períodos de alta demanda.

9.2. A contratada deverá implementar mecanismo de controle de taxa de requisições (rate limiting) configurável, prevenindo abusos e garantindo estabilidade do serviço.

9.3. O limite de requisições simultâneas, por minuto ou hora, deverá ser acordado com a contratante com base em estudo de volume esperado, podendo ser revisado durante a execução contratual conforme crescimento da demanda.

10. ATUALIZAÇÕES E EVOLUÇÕES

10.1. A contratada deverá manter a API atualizada com foco na:

- Correção de erros identificados;
- Inclusão de melhorias tecnológicas e de segurança;
- Atendimento a novas demandas funcionais apresentadas pela contratante.

10.2. Correções consideradas críticas, que afetam diretamente o funcionamento ou a segurança da solução, deverão ser implementadas no prazo máximo de 48 (quarenta e oito) horas após sua identificação e validação.

10.3. Toda atualização deverá ser precedida de comunicação formal à contratante, com informações técnicas sobre impactos, prazos e procedimentos de transição.

11. DISPOSIÇÕES FINAIS

11.1. A empresa contratada será responsável integral 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.

11.2. Todas as obrigações técnicas descritas neste Anexo deverão ser observadas e implementadas pela contratada durante toda a vigência do contrato, sendo vedada a 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 Polícia Federal com antecedência mínima de 5 (cinco) dias úteis, acompanhada da devida 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 de 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 Polícia Federal, quando aplicáveis.

11.6. As funcionalidades da API e os dados fornecidos deverão atender às necessidades operacionais, administrativas e estratégicas da Polícia Federal, de modo a permitir 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 Polícia Federal, por meio de canal oficial 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, 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 Administração, estando compreendidas no escopo da prestação continuada dos serviços contratados. A contratante poderá solicitar a substituição de consultores ou a redistribuição das horas conforme as demandas técnicas evoluam, desde que mantido o saldo contratado.



Documento assinado eletronicamente por **VINICIUS TESSINARI DE CARVALHO**, **Chefe de Divisão**, em 17/07/2025, às 13:30, 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?](https://sei4.pf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=95044229&crc=62829C4D)

[acao=documento_conferir&id_orgao_acesso_externo=0&cv=95044229&crc=62829C4D.](https://sei4.pf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=95044229&crc=62829C4D)

Código verificador: **95044229** e Código CRC: **62829C4D**.