DIÁRIO OFICIAL DA UNIÃO

Publicado em: 06/11/2026 | Edição: 209-B | Seção: 1 - Extra B | Página: 10

Órgão: Ministério dos Transportes/Secretaria Nacional de Trânsito

PORTARIA Nº 971, DE 5 DE NOVEMBRO DE 2026

Estabelece os requisitos técnicos e os procedimentos para homologação e utilização de soluções tecnológicas de guarda monitorada de veículos, nos termos da Resolução Contran nº 1.025, de 26 de junho de 2026.

O SECRETÁRIO NACIONAL DE TRÂNSITO, no uso das atribuições que lhe conferem o art. 19, incisos I, II, V e XIV, da Lei nº 9.503, de 23 de setembro de 1997 - Código de Trânsito Brasileiro, e os arts. 2º, §§ 1º a 3º, 3º, incisos I, II, III e V, e 17, § 4º, da Resolução nº 1.025, de 26 de junho de 2026, do Conselho Nacional de Trânsito - Contran, e com base no que consta do Processo Administrativo nº 50000.059972/2026-26, resolve:

Objeto e âmbito de aplicação

Art. 1º Esta Portaria estabelece os requisitos técnicos, os procedimentos de homologação e as condições operacionais de utilização das soluções tecnológicas de guarda monitorada de veículos, de que trata o art. 17 da Resolução Contran nº 1.025, de 26 de junho de 2026.

Parágrafo único. As especificações técnicas e os critérios de verificação de conformidade constam do Anexo desta Portaria.

Art. 2º A utilização de solução tecnológica de guarda monitorada é facultativa aos órgãos ou entidades competentes e depende de prévia homologação da solução pela Secretaria Nacional de Trânsito - Senatran.

§ 1º A autorização da guarda monitorada em cada caso compete ao órgão ou entidade responsável pela aplicação da medida administrativa de remoção, observados os requisitos do art. 17, § 1º, da Resolução Contran nº 1.025, de 2026, e as diretrizes operacionais por ele estabelecidas.

§ 2º A homologação da solução tecnológica não constitui autorização ou credenciamento da pessoa jurídica responsável para prestar serviços de remoção ou guarda de veículos, nem substitui os procedimentos de seleção e contratação aplicáveis aos órgãos ou entidades competentes.

Homologação das soluções tecnológicas

Art. 3º O requerimento de homologação será apresentado à Senatran por meio do sistema Credencia, pelo órgão ou entidade responsável pelo desenvolvimento da solução ou pela pessoa jurídica que a disponibilize, acompanhado de:

I - identificação do requerente, com inscrição no Cadastro Nacional da Pessoa Jurídica - CNPJ, quando aplicável, e indicação de representante e de responsável técnico;

II - identificação da solução, de sua versão, dos componentes tecnológicos e dos modelos de dispositivos compatíveis;

III - descrição da arquitetura, das funcionalidades, dos fluxos de dados, da infraestrutura e dos mecanismos de monitoramento e segurança;

IV - relatório de ensaios e laudo técnico de conformidade com os requisitos do Anexo;

V - documentação das interfaces, dos registros operacionais e dos mecanismos de exportação de dados; e

VI - indicação dos canais de suporte técnico e dos procedimentos para tratamento de falhas e incidentes.

Parágrafo único. A documentação de que trata o caput destina-se à avaliação da solução tecnológica e da capacidade de sua operação e manutenção, não constituindo habilitação econômico-financeira da pessoa jurídica requerente.

Art. 4º O procedimento de homologação observará duas etapas:

I - verificação da conformidade técnica da solução com os requisitos do Anexo; e

II - verificação da interoperabilidade com o Sistema Integrado de Veículos Custodiados - Sivec, conforme as especificações técnicas disponibilizadas pela Senatran.

§ 1º A etapa prevista no inciso I do caput compreende análise documental e poderá incluir diligências, demonstrações funcionais, inspeções técnicas e execução de testes em ambiente de homologação.

§ 2º A etapa prevista no inciso II do caput será exigível somente após a disponibilização, pela Senatran, dos ambientes, das interfaces e da documentação técnica necessários à realização dos testes de integração.

§ 3º Enquanto não forem disponibilizados os meios previstos no § 2º, a solução poderá ser homologada e utilizada com fundamento na aprovação da etapa prevista no inciso I do caput, sem prejuízo da obrigação posterior de demonstrar sua interoperabilidade.

Art. 5º A Senatran poderá solicitar a complementação da documentação, o saneamento de inconformidades ou a repetição de ensaios necessários à verificação dos requisitos técnicos.

§ 1º O requerente terá trinta dias, contados da comunicação eletrônica, para atender à solicitação, admitida uma prorrogação por igual período mediante justificativa.

§ 2º O prazo para análise ficará suspenso enquanto estiver pendente o atendimento à solicitação.

§ 3º O não atendimento da solicitação no prazo estabelecido poderá ensejar o indeferimento do requerimento, sem prejuízo da apresentação de novo pedido.

§ 4º A análise do requerimento será concluída em até sessenta dias, contados do protocolo da documentação completa, descontados os períodos de suspensão previstos no § 2º.

Art. 6º Concluídas as etapas exigíveis e verificado o atendimento dos requisitos técnicos, a Senatran homologará a solução por ato específico, com publicação no Diário Oficial da União e disponibilização da relação de soluções homologadas em seu sítio eletrônico.

§ 1º O ato de homologação identificará a solução, sua versão de referência, a pessoa jurídica ou o órgão responsável e, quando necessário, as configurações e os dispositivos abrangidos.

§ 2º A homologação terá validade de cinco anos, condicionada à manutenção das características técnicas que fundamentaram sua concessão.

§ 3º O pedido de renovação será apresentado pelo sistema Credencia com antecedência mínima de sessenta dias do término da validade, acompanhado de relatório técnico atualizado de conformidade.

Art. 7º As alterações que modifiquem funcionalidades essenciais de monitoramento, dispositivos abrangidos, mecanismos de integridade dos registros, arquitetura de segurança ou interfaces de interoperabilidade dependerão de avaliação da Senatran antes de sua utilização no âmbito da guarda monitorada.

§ 1º As demais atualizações serão comunicadas por meio do Credencia no prazo de trinta dias, com indicação da versão, das alterações realizadas e das evidências de preservação da conformidade.

§ 2º A Senatran poderá determinar a realização de novos testes quando a atualização puder afetar requisito estabelecido nesta Portaria.

Art. 8º O responsável pela solução homologada deverá manter:

I - canal de comunicação técnica atualizado perante a Senatran e os órgãos ou entidades usuários;

II - condições de suporte, atualização, correção de falhas e preservação dos registros gerados;

III - documentação técnica correspondente à versão em utilização; e

IV - mecanismos de comunicação de indisponibilidades e incidentes que comprometam o monitoramento ou a integridade dos registros.

Parágrafo único. Incidentes críticos que comprometam o acompanhamento de veículos submetidos à guarda monitorada serão comunicados aos órgãos ou entidades afetados imediatamente após sua detecção e à Senatran em até vinte e quatro horas, com identificação do impacto, das medidas de contenção e das providências de recuperação.

Art. 9º A Senatran poderá realizar verificações de conformidade durante a validade da homologação e solicitar os registros, os resultados de ensaios e as evidências técnicas necessários à avaliação.

§ 1º As verificações de conformidade poderão compreender inspeções técnicas, auditorias dos componentes da solução, avaliação de configurações, execução de testes e, quando indispensável à comprovação dos requisitos técnicos, exame do código-fonte e de outros elementos de sua arquitetura, assegurada a proteção das informações sujeitas a sigilo legal.

§ 2º Constatado descumprimento dos requisitos de homologação, o responsável será notificado para prestar esclarecimentos e promover as adequações necessárias, podendo a homologação ser suspensa ou cancelada mediante decisão fundamentada em processo administrativo, assegurados o contraditório e a ampla defesa.

Interoperabilidade com o Sivec

Art. 10. As soluções tecnológicas de guarda monitorada deverão permitir a transmissão ao Sivec dos registros de autorização, ativação, acompanhamento, ocorrências e encerramento, observados os leiautes, protocolos, mecanismos de autenticação e procedimentos de integração estabelecidos pela Senatran.

§ 1º A interoperabilidade observará a arquitetura nacional de integração do Sivec.

§ 2º A homologação da interoperabilidade será demonstrada por testes em ambiente disponibilizado pela Senatran, com confirmação de recebimento, tratamento de falhas, prevenção de duplicidade e rastreabilidade das transmissões.

§ 3º Após a disponibilização da integração com o Sivec, as informações relativas à remoção, à guarda monitorada e à situação do veículo poderão ser disponibilizadas nos canais eletrônicos definidos pela Senatran, observados os requisitos de segurança da informação e proteção de dados pessoais aplicáveis.

Procedimentos operacionais

Art. 11. O órgão ou entidade competente que optar pela utilização da guarda monitorada deverá adotar solução previamente homologada pela Senatran e estabelecer os procedimentos internos de autorização, fiscalização e atendimento das ocorrências.

Parágrafo único. A decisão sobre a utilização da guarda monitorada em cada caso e as providências decorrentes de seu acompanhamento permanecerão sob responsabilidade do órgão ou entidade competente, mediante atuação dos agentes e autoridades por ele designados.

Art. 12. A solução tecnológica deverá permitir o registro das informações relativas à guarda monitorada autorizada pelo órgão ou entidade competente, vinculadas ao respectivo Termo de Recolhimento do Veículo, contendo, no mínimo:

I - identificação do órgão ou entidade competente e do agente responsável pelo registro;

II - identificação do veículo e do Termo de Recolhimento do Veículo;

III - identificação do proprietário ou possuidor legítimo responsável pela guarda, quando disponível ao órgão competente;

IV - identificação da solução homologada e do dispositivo utilizado;

V - local autorizado de guarda e parâmetros de monitoramento fixados pelo órgão ou entidade competente;

VI - data e hora da autorização e da ativação do monitoramento; e

VII - registro da ciência do responsável quanto às condições operacionais estabelecidas para a guarda monitorada.

Parágrafo único. A solução deverá permitir o registro das condições autorizadas de deslocamento até o local de guarda, quando necessárias à execução da medida.

Art. 13. A ativação do monitoramento dependerá da vinculação do dispositivo ao veículo, da verificação de seu funcionamento e da confirmação do recebimento dos dados pela solução tecnológica.

§ 1º A instalação, ativação e identificação do dispositivo deverão produzir registros verificáveis, inclusive da data, hora, responsável pela operação e estado inicial do equipamento.

§ 2º A solução deverá impedir a confirmação de ativação quando não houver evidência de comunicação e localização válidas, ressalvadas as hipóteses de contingência expressamente previstas no Anexo.

Art. 14. Durante a guarda monitorada, a solução deverá registrar as informações de localização, integridade do dispositivo, disponibilidade da comunicação e demais eventos necessários à verificação das condições estabelecidas pelo órgão ou entidade competente.

§ 1º Os eventos indicativos de possível descumprimento serão comunicados automaticamente ao órgão ou entidade competente, com os respectivos registros técnicos e elementos necessários à sua verificação.

§ 2º Os eventos decorrentes de perda de sinal, imprecisão de posicionamento ou falha técnica serão identificados de forma distinta dos eventos de movimentação ou violação confirmados pelos mecanismos da solução.

§ 3º A geração de alerta tecnológico não substitui a avaliação do órgão ou entidade competente quanto à ocorrência de descumprimento e à adoção das providências previstas no art. 17, § 3º, da Resolução Contran nº 1.025, de 2026.

Art. 15. O encerramento do monitoramento dependerá de registro realizado ou autorizado pelo órgão ou entidade competente, observadas as hipóteses e os procedimentos aplicáveis à liberação, ao recolhimento físico ou à destinação do veículo.

Parágrafo único. A solução deverá preservar o histórico da autorização, das ocorrências, das alterações de parâmetros, da desativação e da retirada do dispositivo, com identificação dos responsáveis e respectivas datas e horas.

Disposições transitórias e finais

Art. 16. Após a disponibilização dos meios técnicos necessários à integração com o Sivec, a Senatran convocará os responsáveis pelas soluções anteriormente homologadas para demonstrar sua interoperabilidade, no prazo de cento e oitenta dias, contado da convocação.

§ 1º O prazo poderá ser prorrogado uma vez, por até sessenta dias, mediante justificativa técnica aceita pela Senatran.

§ 2º A obrigação de integração pressupõe a disponibilização pela Senatran de documentação técnica, ambiente de testes e interfaces operacionais necessários à sua execução.

§ 3º O descumprimento do prazo sujeitará a solução aos procedimentos de verificação e às medidas previstas no art. 9º, sem prejuízo da preservação dos registros produzidos durante o período anterior.

§ 4º Os responsáveis pelas soluções tecnológicas homologadas deverão preservar integralmente, desde o início de sua utilização, os registros de monitoramento e os dados de telemetria de localização coletados durante a guarda monitorada, inclusive aqueles produzidos anteriormente à disponibilização da integração com o Sivec, observados os requisitos de segurança e retenção estabelecidos no Anexo.

§ 5º Após a disponibilização da integração com o Sivec, a Senatran poderá determinar a transmissão dos registros históricos de que trata o § 4º, observados os leiautes, os procedimentos e os prazos estabelecidos na documentação técnica de interoperabilidade.

Art. 17. A Senatran disponibilizará documentação e manuais técnicos de interoperabilidade com o Sivec, destinados à implementação dos requisitos previstos nesta Portaria e em seu Anexo.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

ADRUALDO DE LIMA CATÃO

ANEXO

1. REQUISITOS GERAIS DA SOLUÇÃO

1.1. A solução deverá compreender os componentes necessários ao cadastro da autorização do órgão ou entidade competente, à associação do dispositivo ao veículo, ao monitoramento, ao tratamento de eventos, à consulta pelos órgãos competentes e à exportação de registros.

1.2. Deverá identificar de forma unívoca cada autorização de guarda monitorada, o veículo, o dispositivo utilizado e a versão da solução que gerou os registros.

1.3. Deverá permitir a operação por diferentes órgãos ou entidades, com segregação lógica de dados, de usuários e de permissões, quando utilizada em ambiente compartilhado.

1.4. Deverá disponibilizar, ao órgão ou entidade competente, consulta autenticada aos veículos sob acompanhamento, à situação dos dispositivos, aos alertas pendentes e ao histórico das ocorrências.

1.5. Deverá manter os registros com data e hora padronizadas, referência ao fuso horário e mecanismos de sincronização de relógios que permitam correlacionar eventos de diferentes componentes.

1.6. Deverá conservar evidências de alterações de configuração, substituição de dispositivo e mudança dos parâmetros de monitoramento, sem eliminar o histórico anterior.

1.7. Deverá assegurar o recebimento automático de registros produzidos durante períodos de indisponibilidade de conectividade, preservada a ordem lógica e a identificação da data e hora originais de cada evento.

1.8. Deverá permitir consulta e exportação de registros em formato aberto, estruturado e documentado, sem dependência exclusiva de interface visual ou relatório em formato fechado.

1.9. A arquitetura deverá ser documentada, com identificação dos componentes de coleta, comunicação, processamento, armazenamento, auditoria, contingência e integração.

1.10. As interfaces da solução tecnológica destinadas aos usuários, inclusive proprietários ou possuidores legítimos dos veículos, deverão observar os critérios de acessibilidade estabelecidos nas Diretrizes de Acessibilidade para Conteúdo Web (Web Content Accessibility Guidelines - WCAG), versão 2.2, nível AA, do World Wide Web Consortium - W3C, no que forem aplicáveis.

1.11. A solução tecnológica deverá disponibilizar interface eletrônica destinada ao proprietário ou possuidor legítimo responsável pela guarda monitorada, que permita consultar, no mínimo, a situação do monitoramento, o local autorizado de guarda, as condições operacionais estabelecidas e as ocorrências relacionadas ao veículo.

1.12. A solução tecnológica deverá dispor de mecanismos de notificação ativa ao proprietário ou possuidor legítimo responsável pela guarda monitorada, por meio eletrônico, contemplando, no mínimo:

1.12.1. o início e o encerramento do monitoramento;

1.12.2. a identificação de eventos indicativos de descumprimento das condições da guarda monitorada;

1.12.3. a ocorrência de falhas ou indisponibilidades que demandem providências do responsável; e

1.12.4. outras ocorrências operacionais definidas pelo órgão ou entidade competente.

1.13. As notificações deverão possuir registro da data e hora de geração, do meio utilizado, do resultado da tentativa de envio e, quando disponível, da confirmação de entrega, sem substituir as comunicações ou notificações administrativas legalmente exigidas.

2. DISPOSITIVOS DE MONITORAMENTO E GEOLOCALIZAÇÃO

2.1. O dispositivo deverá possuir identificador único e permanente, passível de conferência física ou eletrônica e vinculação à autorização de guarda monitorada.

2.2. A localização deverá ser obtida por sistema de posicionamento por satélite ou tecnologia equivalente, com registro das coordenadas, data e hora da aferição e indicador de qualidade ou precisão disponível.

2.3. O conjunto dispositivo e solução deverá demonstrar, em ensaio sob condições de céu aberto, erro horizontal não superior a trinta metros em pelo menos noventa e cinco por cento das amostras válidas, sem prejuízo do registro de situações de degradação do sinal.

2.4. Em deslocamento, o intervalo entre amostras de posição não deverá superar sessenta segundos durante período de comunicação disponível; com o veículo estacionado, o intervalo não deverá superar cinco minutos.

2.5. O dispositivo deverá detectar e registrar, conforme sua arquitetura, desligamento, perda de alimentação, remoção, abertura, violação, interferência no sinal ou outra condição técnica que comprometa o monitoramento.

2.6. O sistema deverá distinguir eventos detectados diretamente pelo dispositivo daqueles inferidos a partir da perda de comunicação ou da ausência de dados.

2.7. A comunicação sem fio sujeita à regulamentação de telecomunicações deverá utilizar módulos com certificação aplicável da Agência Nacional de Telecomunicações - Anatel.

2.8. O requerente deverá demonstrar, para cada modelo de dispositivo, as condições de alimentação, a autonomia energética estimada, a periodicidade de coleta e transmissão dos dados e o comportamento em situações de perda de energia ou comunicação, considerando as diferentes condições de operação.

2.9. A substituição de dispositivo deverá gerar novo vínculo, com registro da justificativa, do responsável e dos identificadores anterior e posterior.

2.10. A solução não poderá depender de recurso de bloqueio remoto de ignição ou de imobilização do veículo para atendimento aos requisitos desta Portaria.

2.11. A solução deverá possuir mecanismos de acompanhamento da disponibilidade energética do dispositivo de monitoramento, com geração de alertas preventivos quando identificada condição que possa comprometer a continuidade do monitoramento, permitindo a adoção tempestiva das medidas necessárias à manutenção de seu funcionamento.

2.12. A continuidade do monitoramento poderá ser assegurada mediante recarga, substituição ou manutenção do dispositivo, observadas as características da tecnologia utilizada e os procedimentos estabelecidos pelo órgão ou entidade competente, devendo todas as intervenções ser registradas de forma rastreável.

3. MONITORAMENTO, CERCAMENTO GEOGRÁFICO E ALERTAS

3.1. A solução deverá permitir configurar, por autorização, a área de permanência do veículo, o período de vigência do monitoramento e as condições de deslocamento expressamente autorizadas pelo órgão ou entidade competente.

3.2. A cerca virtual deverá admitir representação geográfica verificável e manter histórico das alterações de limites, responsáveis e momentos de vigência.

3.3. O processamento dos eventos deverá considerar a qualidade do posicionamento e a margem de incerteza da medição, de modo a não caracterizar automaticamente como violação um ponto isolado de baixa confiabilidade.

3.4. A solução deverá gerar registros distintos, no mínimo, para: saída da área autorizada; deslocamento não autorizado; possível remoção ou violação do dispositivo; perda de alimentação; interrupção de comunicação; recuperação de comunicação; alteração de configuração; e encerramento do monitoramento.

3.5. Os alertas decorrentes de dados regularmente recebidos deverão ser disponibilizados ao órgão ou entidade competente em tempo real, imediatamente após sua identificação pelo sistema.

3.6. A ausência de comunicação do dispositivo por período superior a dez minutos deverá gerar alerta específico de perda de comunicação, sem ser classificada automaticamente como deslocamento ou violação física.

3.7. Os registros de posição e de eventos coletados durante indisponibilidade de comunicação deverão ser preservados localmente e retransmitidos automaticamente após o restabelecimento da conexão, respeitada a capacidade declarada e comprovada do dispositivo.

3.8. Os alertas deverão conter identificador do evento, autorização e dispositivo associados, data e hora da ocorrência e do recebimento, classificação, dados técnicos que o fundamentaram e situação de tratamento pelo órgão competente.

3.9. A solução deverá permitir registrar ciência, análise e providências adotadas pelo órgão ou entidade competente, sem alterar ou eliminar o evento original.

3.10. A geração de eventos e alertas deverá ser testada em cenários de deslocamento, imobilidade, alteração de cerca virtual, degradação de posicionamento, desligamento do dispositivo e interrupção e recuperação da conectividade.

4. SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

4.1. O acesso de usuários deverá utilizar credenciais individuais, perfis segregados por função e concessão de permissões estritamente necessárias às atividades desempenhadas.

4.2. Os perfis administrativos e os perfis com autorização para alteração de parâmetros de monitoramento deverão utilizar autenticação de múltiplos fatores.

4.3. Os dados deverão ser protegidos por criptografia em trânsito e em repouso, mediante algoritmos e configurações atualizados, documentados e compatíveis com padrões técnicos reconhecidos.

4.4. Os registros operacionais e as trilhas de auditoria deverão possuir controles de integridade que permitam identificar alteração, supressão, inserção ou reordenação não autorizada.

4.5. A trilha de auditoria deverá registrar, no mínimo, identidade do usuário ou componente, operação, objeto afetado, data e hora, origem de acesso, resultado e referência à versão da solução.

4.6. Os registros de auditoria deverão ser protegidos contra alteração e exclusão pelos usuários operacionais, inclusive aqueles com privilégios administrativos ordinários.

4.7. A solução deverá manter registros de acesso, monitoramento e ocorrências pelo período necessário à fiscalização, assegurada retenção dos registros operacionais e de telemetria por cinco anos após o encerramento da guarda monitorada, ressalvados prazos superiores legalmente aplicáveis.

4.8. Quando operada para mais de um órgão ou entidade, deverá ser demonstrado, por testes, que usuários de um órgão não podem consultar ou alterar dados pertencentes a outro, ressalvadas permissões expressamente autorizadas.

4.9. Deverão existir procedimentos documentados para gestão de vulnerabilidades, atualização de componentes, cópias de segurança, restauração de dados, recuperação de incidentes e continuidade do serviço.

4.10. A solução deverá aplicar mecanismos de minimização dos dados pessoais tratados, de registro do acesso a esses dados e de controle de sua exportação, mantendo-os vinculados às finalidades de guarda monitorada.

4.11. As evidências de auditoria e os registros exportados deverão preservar identificação da origem, integridade verificável, período de abrangência e cadeia de eventos necessária à reconstituição técnica.

5. REGISTROS OPERACIONAIS, DADOS E RASTREABILIDADE

5.1. O registro inicial deverá conter os dados previstos no art. 12 desta Portaria e as informações do Termo de Recolhimento do Veículo necessárias à identificação e à rastreabilidade da medida, observando o art. 14 da Resolução Contran nº 1.025, de 2026.

5.2. Cada registro de posição deverá conter identificador da autorização e do dispositivo, data e hora da medição, coordenadas geográficas, informação disponível sobre qualidade da posição e indicação do estado da comunicação.

5.3. Cada evento deverá possuir identificador único, categoria, data e hora de ocorrência, origem da detecção, evidências vinculadas, condição de recebimento e histórico de tratamento.

5.4. A alteração de perímetro, prazo, responsável pela operação ou estado da autorização dependerá da identificação de usuário habilitado e deverá ser registrada com preservação do valor anterior.

5.5. A solução deverá disponibilizar relatórios e extrações de autorizações vigentes e encerradas, dispositivos vinculados, eventos, indisponibilidades e histórico de alterações.

5.6. A disponibilização de dados ao órgão ou entidade competente deverá ocorrer por meio autenticado, com rastreabilidade do acesso e possibilidade de extração em formato estruturado.

5.7. Os arquivos que constituam evidência técnica deverão possuir identificador, metadados de geração e mecanismo de verificação de integridade.

5.8. Os dados coletados deverão ser limitados àqueles necessários à execução da guarda monitorada, à sua supervisão e à eventual apuração de descumprimentos.

6. DOCUMENTAÇÃO, ENSAIOS E COMPROVAÇÃO DE CONFORMIDADE

6.1. O requerimento de homologação deverá ser instruído com memorial descritivo da solução, diagramas de arquitetura e comunicação, inventário dos componentes, matriz de requisitos e identificação das versões submetidas aos ensaios.

6.2. O laudo técnico deverá indicar, para cada requisito do Anexo, o procedimento de verificação, o resultado obtido, as evidências produzidas e a conclusão de conformidade ou não conformidade.

6.3. O laudo deverá ser emitido por profissional ou instituição com capacidade técnica demonstrável e independência em relação às atividades de desenvolvimento da versão avaliada, admitidas instituições públicas e universidades.

6.4. Os ensaios deverão abranger, no mínimo, funcionamento da autorização e da ativação, vinculação e substituição do dispositivo, precisão e periodicidade de localização, geração de alertas, perda e recuperação de comunicação, trilhas de auditoria, controle de acesso, exportação e integridade dos registros.

6.5. Os testes de geolocalização deverão descrever método, quantidade de amostras, condições ambientais e critérios para descarte de medições inválidas, permitindo a reprodução dos resultados.

6.6. Os testes de segurança deverão incluir avaliação de permissões, segregação de dados, proteção de interfaces, mecanismos criptográficos, preservação dos registros e recuperação de cópias de segurança.

6.7. O requerente deverá demonstrar a capacidade da solução para o volume simultâneo de autorizações declarado, com medição de processamento, disponibilidade e tempo de entrega de alertas.

6.8. Deverão ser apresentados procedimentos de suporte, gestão de incidentes, continuidade operacional, controle de versões e manutenção dos dispositivos compatíveis com o funcionamento declarado.

6.9. A Senatran poderá solicitar demonstrações assistidas, testes complementares e inspeções técnicas, inclusive acesso aos componentes, às configurações, aos registros, à documentação e ao código-fonte da solução, quando indispensáveis à verificação de conformidade, mediante procedimentos que assegurem a confidencialidade e a proteção das informações examinadas.

6.9.1. O exame do código-fonte poderá ser realizado em ambiente computacional controlado, inclusive mediante acesso remoto seguro, com mecanismos de restrição de cópia e transferência de informações, limitado aos componentes necessários à auditoria.

6.10. O responsável deverá manter disponíveis os relatórios de ensaio, as evidências de conformidade e a documentação das versões homologadas durante a validade da homologação.

7. INTEROPERABILIDADE COM O SIVEC

7.1. A solução deverá possuir interface documentada que permita integração com o Sivec, observada a arquitetura e os padrões de segurança definidos pela Senatran.

7.2. Deverá permitir a transmissão estruturada ao Sivec dos registros de autorização, de ativação, de alteração dos parâmetros autorizados, da totalidade dos dados de telemetria de localização do veículo coletados durante o período de guarda monitorada, das ocorrências relevantes, da substituição do dispositivo e do encerramento da guarda monitorada.

7.3. Cada transmissão deverá possuir identificador unívoco, data e hora do evento original, identificação do remetente e mecanismo de confirmação de recebimento.

7.4. A solução deverá controlar tentativas de envio, reenvio após falha, tratamento de rejeições, prevenção de duplicidades e reconciliação de eventos pendentes.

7.5. A interoperabilidade deverá preservar a integridade e a rastreabilidade dos registros, inclusive quando houver transmissão posterior à ocorrência por indisponibilidade temporária de conexão.

7.6. O requerente deverá demonstrar os fluxos de integração em ambiente de homologação, com execução de cenários de sucesso, rejeição, indisponibilidade, reenvio e recuperação.

7.7. Os leiautes, protocolos de autenticação, endereços técnicos, esquemas de mensagens, códigos de eventos e demais parâmetros de implementação observarão a documentação disponibilizada pela Senatran, sem afastar os requisitos estabelecidos nesta Portaria.

7.8. A transmissão dos dados de telemetria de localização ao Sivec deverá abranger a integralidade dos registros de posicionamento geográfico coletados durante a guarda monitorada, incluindo, no mínimo, a identificação da autorização e do dispositivo de monitoramento, as coordenadas geográficas, a data e hora de cada registro e as informações disponíveis sobre a precisão do posicionamento, observando-se a periodicidade, a frequência de envio, os protocolos e os demais parâmetros estabelecidos nos padrões e manuais técnicos de interoperabilidade da Senatran.

7.9. A solução deverá assegurar a preservação e a transmissão integral dos registros de telemetria de localização, inclusive daqueles coletados durante períodos de indisponibilidade de comunicação, mediante mecanismos de armazenamento temporário, reenvio automático, confirmação de recebimento e prevenção de duplicidades, de forma a garantir a integridade, a continuidade e a rastreabilidade das informações transmitidas ao Sivec.

7.10. A solução deverá permitir a extração e a transmissão ao Sivec da integralidade dos registros históricos de monitoramento e de telemetria de localização, inclusive aqueles produzidos anteriormente à implantação da interoperabilidade, preservados os identificadores originais, as datas e horas dos eventos, a integridade dos registros e os mecanismos de controle de duplicidade.

Acessível com VLibras

Este conteúdo não substitui o publicado na versão certificada.