VIII – certidão negativa de falência, expedida pelo distribuidor da sede da pessoa jurídica, com data inferior a 60 (sessenta) dias, contada da data de protocolo do requerimento;

IX – declaração de que não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do art. 7º da Constituição Federal e do art. 68, inciso VI, da Lei Federal nº 14.133, de 1º de abril de 2021; e

X – escritura pública declaratória dos sócios e administradores da pessoa jurídica requerente quanto ao não exercício de atividades empresariais relacionadas à vistoria veicular, à venda ou revenda de bases de dados e informações veiculares, e de que a pessoa jurídica requerente não tenha sofrido sanção de cassação de credenciamento de qualquer atividade há menos de 2 (dois) anos, imposta por qualquer órgão público.

Art. 27. A pessoa jurídica requerente deverá comprovar, na fase de análise documental, perante o NUCON, o cumprimento dos requisitos relativos à tecnologia da informação, à qualificação técnica, à qualificação profissional, à segurança da informação, à proteção de dados pessoais, à continuidade operacional e às demais exigências documentais previstas nesta Portaria, bem como apresentar toda a documentação pertinente aos itens abaixo:

I – descrição detalhada da solução tecnológica a ser homologada, contendo sua arquitetura, funcionalidades, módulos, integrações, recursos de segurança, fluxos operacionais, mecanismos de auditoria, rastreabilidade e documentação técnica pertinente;

II – sistema de gestão da qualidade certificado na norma ABNT NBR ISO 9001, com validade atestada por entidade certificadora acreditada pelo INMETRO ou signatária de acordos internacionais de reconhecimento mútuo no campo da acreditação, com escopo compatível com as atividades relacionadas ao objeto da homologação;

III – sistema de gestão de segurança da informação certificado na norma ABNT NBR ISO/IEC 27001, com validade atestada por entidade certificadora acreditada pelo INMETRO ou signatária de acordos internacionais de reconhecimento mútuo no campo da acreditação, com escopo compatível com as atividades relacionadas ao objeto da homologação;

IV – sistema de gestão da continuidade de negócios na forma da norma ABNT NBR ISO 22301, com validade atestada por entidade certificadora acreditada pelo INMETRO ou signatária de acordos internacionais de reconhecimento mútuo no campo da acreditação;

V – certificação de compliance PCI DSS, nível 2, visando à proteção dos dados relativos ao pagamento eletrônico;

VI – certificação e atendimento à norma ABNT NBR ISO 20000, com validade atestada por entidade certificadora acreditada pelo INMETRO ou signatária de acordos internacionais de reconhecimento mútuo no campo da acreditação;

VII – certificação de conformidade com normas técnicas, devendo o sistema auditor possuir certificação ISO/IEC 12207, relativa a processos de ciclo de vida do software, e ISO 29119, relativa a testes de software;

VIII – certificação de proteção de dados pessoais na nuvem, devendo o sistema auditor possuir certificação ISO/IEC 27018;

IX – certificação de Sistemas de Gestão de Inteligência Artificial (SGIA) – ISO 42001/2024;

X – atestado de capacidade técnica emitido por entidade pública ou privada, atestando que a pessoa jurídica requerente é responsável pelo desenvolvimento e manutenção de solução tecnológica cuja finalidade seja o registro e monitoramento de vistorias de identificação veicular regulamentadas por departamentos estaduais de trânsito, com utilização de inteligência artificial e contendo as validações dispostas nesta Portaria;

XI – atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado que comprove que a empresa executou a prestação de serviços de intermediação de pagamentos;

XII – comprovação de possuir em seu corpo técnico, no mínimo, um profissional responsável pela administração de bancos de dados (DBA), com certificação na solução de banco de dados utilizada na solução objeto de auditoria, em sua versão vigente;

XIII – comprovação de possuir em seu corpo técnico, no mínimo, um profissional responsável pela administração da infraestrutura de tecnologia da informação, com certificação profissional na solução de servidores de aplicação utilizada na solução objeto de auditoria, em sua versão vigente; e

XIV – comprovação de possuir em seu corpo técnico, no mínimo, um profissional com formação de nível superior em engenharia, responsável pela administração dos sistemas informatizados que compõem a solução objeto de auditoria.

§ 1º Os sistemas de gestão a que se referem os incisos II a IX deste artigo deverão estar acompanhados, na fase de análise documental, dos seguintes documentos: certificado e relatório da última auditoria realizada pela entidade certificadora, relatório da última auditoria interna e análise crítica da alta direção do respectivo sistema.

§ 2º Os atestados de capacidade técnica a que se referem os incisos X e XI deste artigo deverão estar acompanhados de contratos de prestação de serviços e de notas fiscais que demonstrem a efetiva prestação dos serviços às empresas que executam a atividade de vistoria veicular do Estado emissor do respectivo atestado.

§ 3º A comprovação dos profissionais de que tratam os incisos XII, XIII e XIV deste artigo deverá ser realizada por meio de documentação idônea que evidencie o vínculo profissional com a pessoa jurídica requerente, inclusive contrato social, carteira de trabalho, contrato de prestação de serviços ou outro instrumento juridicamente válido.

§ 4º A pessoa jurídica requerente deverá apresentar, na fase de análise documental, Relatório de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) como requisito para homologação inicial, bem como mantê-lo atualizado sempre que houver alteração relevante de escopo, inclusive implantação ou modificação de módulos de Inteligência Artificial, autenticação biométrica, geolocalização, novas integrações, ampliação de base de dados ou mudança relevante nas finalidades, categorias de dados tratados ou riscos aos titulares.

§ 5º A pessoa jurídica requerente deverá apresentar, na fase de análise documental, os planos de continuidade, com RTO e RPO homologados, backup on-site e off-site, WAF, IDS/IPS, mitigação DDoS e evidências de testes periódicos de contingência, sem prejuízo de sua posterior verificação prática na etapa de avaliação de conformidade, devendo os incidentes relevantes de segurança da informação ou de proteção de dados pessoais ser comunicados ao DETRAN/CE em até 24 (vinte e quatro) horas da ciência, com relatório circunstanciado em até 72 (setenta e duas) horas, sem prejuízo das comunicações ao encarregado pelo tratamento de dados e à Autoridade Nacional de Proteção de Dados – ANPD, quando cabíveis.

Art. 28. A pessoa jurídica requerente deverá comprovar, na fase de análise documental, que dispõe de infraestrutura de datacenter, própria ou de terceiros, apta a suportar a solução tecnológica submetida à homologação, atendendo, no mínimo, às seguintes exigências:

I – hospedagem do software, banco de dados, evidências digitais, imagens, vídeos e demais informações críticas em datacenter classificado, no mínimo, como Tier III, ou padrão técnico equivalente que assegure redundância, alta disponibilidade e tolerância a falhas;

II – infraestrutura redundante, com disponibilidade mínima mensal de 99,0% (noventa e nove por cento);

III – instalações elétricas adequadas, com apresentação de Anotação de Responsabilidade Técnica – ART, bem como sistema alternativo de energia com autonomia mínima de 12 (doze) horas;

IV – ambiente com climatização adequada, segurança física de acesso, sistema de prevenção e combate a incêndio compatível com equipamentos de informática e mecanismos de proteção lógica compatíveis com a criticidade da operação;

V – existência de ambiente secundário, ou solução equivalente de contingência, apto a permitir a retomada do funcionamento da solução em prazo não superior a 2 (duas) horas, em caso de falha do ambiente principal; e

VI – recursos de backup e armazenamento seguro, em ambiente segregado do ambiente de produção, assegurando a guarda, integridade, rastreabilidade e disponibilidade dos dados, evidências, imagens e demais informações tratadas pela solução.

§ 1º Na hipótese de utilização de infraestrutura terceirizada, a pessoa jurídica requerente deverá apresentar declaração formal da empresa prestadora, comprovando a classificação mínima exigida, a vinculação da requerente à infraestrutura utilizada e a responsabilidade solidária quanto à guarda, disponibilidade, integridade e segurança dos dados e evidências armazenados.

§ 2º A comprovação documental de que trata o caput não afasta a possibilidade de verificação prática da infraestrutura e dos mecanismos de continuidade, contingência, segurança e backup na etapa de avaliação de conformidade, quando necessária à validação técnica, operacional e funcional da solução.

Art. 29. A avaliação de conformidade ficará a cargo do NUTIN, com a participação do NUREG e do NUVIS, no âmbito de suas competências finalísticas, e será restrita à validação técnica, operacional e funcional da solução tecnológica, de seus recursos, integrações, mecanismos de segurança, rotinas de captura, inteligência artificial, visão computacional, aderência aos procedimentos de vistoria e demais requisitos práticos de funcionamento previstos nesta Portaria.

I – validação prática de que a solução tecnológica permite ao DETRAN/CE acesso, em tempo real, aos registros, vídeos, imagens, dados, metadados, trilhas de auditoria e laudos vinculados às vistorias realizadas, pelo prazo mínimo de 5 (cinco) anos, para fins de fiscalização, auditoria, rastreabilidade, revisão administrativa e apuração de inconformidades;

II – validação prática de recurso tecnológico que permita a análise crítica das imagens e demais evidências digitais recebidas, inclusive mediante classificação, triagem e organização das informações necessárias à revisão administrativa;

III – validação prática da integração segura com os sistemas, aplicativos, barramentos, APIs, repositórios e demais soluções tecnológicas oficiais do DETRAN/CE;

IV – validação prática de recurso tecnológico que realize o controle de acesso dos usuários ao sistema por meio de autenticação forte, inclusive por identificação biométrica digital ou facial, com rastreabilidade individual, registro de eventos de autenticação e mecanismos de prevenção ao uso compartilhado ou indevido de credenciais;

V – validação prática dos recursos tecnológicos de proteção, na arquitetura de hardware e software, que incluam firewall, sistema automático de detecção de intrusão, sistema de prevenção de intrusão e mecanismos de filtragem e mitigação de ataques de negação de serviço;