



Consulta Pública Eletrônica

Solução de Prova de Vivacidade (LIVENESS)

<https://www.serpro.gov.br/consultas-publicas/sede/0272-2026>

Brasília/DF, março de 2026.



Sumário

Orientações para Resposta à Consulta Pública	2
1. Objeto	6
2. Especificação do Objeto	7
2.1. Solução de Prova de Vivacidade (LIVENESS)	7
2.1.1. Dos Requisitos Funcionais da Solução	7
2.1.2. Dos Requisitos Não Funcionais	12

Orientações para Resposta à Consulta Pública

As empresas interessadas deverão encaminhar resposta à presente Consulta Pública, por meio do endereço eletrônico consulta.publica.supec@serpro.gov.br, contendo, no mínimo, as seguintes informações e documentos:

1. Identificação da empresa

- Razão social e nome fantasia;
- CNPJ;
- Endereço completo;
- Sítio eletrônico institucional.

2. Dados para contato

- Nome completo do responsável pela resposta à Consulta Pública;
- Cargo;
- Telefones para contato;
- Endereço de e-mail.

3. Identificação da solução

- Nome da solução, objeto desta Consulta Pública;
- Nome do fabricante;
- Sítio eletrônico do fabricante da solução.

4. Descrição da solução

- Descrição detalhada da solução e de seus componentes, acompanhada da documentação técnica pertinente, tais como catálogos, datasheets, manuais, brochuras ou documentos equivalentes;
- Checklist de atendimento aos requisitos da solução, indicando, para cada item, se o requisito é atendido integralmente, parcialmente ou não atendido, com as respectivas observações e esclarecimentos;
- Descrição detalhada do(s) modelo(s) de comercialização da solução, contemplando, no mínimo, licenciamento de uso perpétuo, subscrição de software e eventuais outras modalidades existentes;

- Descrição detalhada das métricas de licenciamento da solução.

5. Estudo de preços

Apresentar estudo de preços completo da solução, de forma detalhada e segregada, contemplando, no mínimo:

- **licenciamento de uso perpétuo**, com identificação de SKU/part number, nome do software, métrica de licenciamento, quantitativos considerados, valores unitários e valores totais estimados;
- **subscrição de software**, com identificação de SKU/part number, nome do software, métrica de licenciamento, período de contratação, quantitativos considerados, valores unitários e valores totais estimados;
- descrição de **outras modalidades de comercialização eventualmente existentes**, com os respectivos valores estimados;
- **estimativa dos serviços de implantação**, contemplando as atividades previstas, o esforço estimado, o perfil dos profissionais envolvidos, a quantidade estimada de horas ou homem-hora, o prazo estimado para implantação e entrada em produção da solução, bem como os valores unitários e totais correspondentes;
- **estimativa do tempo necessário para implementação da solução**, considerando, quando aplicável, as etapas de instalação, configuração, integração, parametrização, testes, homologação, treinamento e entrada em produção;
- **estimativa de valores unitários de serviços técnicos especializados**, por hora, para atendimento a necessidades futuras do SERPRO, incluindo, quando possível, a discriminação por perfil profissional ou tipo de serviço técnico especializado;
- demais custos eventualmente associados à solução, inclusive serviços acessórios, treinamento, atualização, manutenção ou outros itens que componham o custo total de propriedade.

6. Base de clientes

- Quantidade de clientes no Brasil;
- Relação de entes públicos que já tenham adquirido a solução.

7. Experiência e suporte técnico

- Informar se o suporte técnico é prestado diretamente pelo fabricante ou por parceiro autorizado;
- Informar os níveis de serviço ofertados para a solução, incluindo, entre outros, prazo de atendimento, prazo de solução, horários de cobertura e canais de atendimento disponíveis.

8. Transferência de conhecimento

- Informar a forma de repasse de conhecimento para operação e sustentação da solução;
- Apresentar resumo das grades de capacitação, conteúdos programáticos e respectivas cargas horárias.

9. Dimensionamento da infraestrutura de hardware

Apresentar estudo da infraestrutura de hardware mais adequada para produção da solução ofertada, considerando, no mínimo, os seguintes aspectos:

- throughput;
- matriz de compatibilidade de hardware e software;
- armazenamento;
- processamento;
- topologia;
- alta disponibilidade.

10. Transparência e Integridade

Todos os documentos e informações relacionados ao processo de contratação do Serpro e desta consulta pública estão disponíveis no portal de transparência:

<https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos>

Regulamento de Licitações e Contratos do Serpro:

<https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/regulamento>

Para este processo foi observado a política de integridade de acordo com art. 32, inc. V, da Lei nº 13.303/2016, Programa Corporativo de Integridade do Serpro – PCINT (TR - 138/2022) e a Cartilha de Integridade do Processo de Aquisições e Contratações.

Para conhecimento das regras de conduta no relacionamento entre fornecedores e empregados do Serpro, acesse a Cartilha de Integridade do Processo de Aquisições e Contratações, disponível no link: https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/cartilha_integridade_paq.pdf

Ressaltamos que o Serpro não concede ou autoriza nenhum tipo de registro de oportunidade em seus processos de contratação.

1. Objeto

O Serviço Federal de Processamento de Dados – Serpro torna pública a presente **Consulta Pública Eletrônica**, no formato *Request for Proposal* (RFP), com a finalidade de identificar soluções tecnológicas, empresas fornecedoras e colher contribuições do mercado visando subsidiar a futura contratação de **Solução de Prova de Vivacidade (LIVENESS)**.

A iniciativa busca soluções tecnológicas de **prova de vivacidade (liveness detection)** que atendam aos mais elevados padrões de **segurança, precisão, desempenho e escalabilidade**, aplicáveis a processos de captura e detecção de prova de vida facial no contexto de serviços digitais ofertados à Administração Pública.

A solução a ser considerada deverá, obrigatoriamente, permitir **integração com os sistemas e aplicações já existentes**, por meio de APIs, SDKs ou outros mecanismos de interoperabilidade, de forma a viabilizar sua incorporação aos fluxos de autenticação digital atualmente em operação.

Deverá ainda assegurar a **proteção de dados biométricos e pessoais**, em conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados (LGPD), bem como garantir a rastreabilidade e auditabilidade das transações realizadas.

Adicionalmente, a solução deverá ser capaz de **mitigar fraudes associadas ao uso indevido de biometria**, incluindo tentativas baseadas em fotos, vídeos, máscaras ou técnicas avançadas como deepfakes, por meio de mecanismos robustos de detecção de vivacidade, preferencialmente com suporte a abordagens passivas e/ou híbridas. Espera-se ainda que a solução apresente **arquitetura moderna, flexível e resiliente**, com capacidade de operação em ambientes escaláveis e de alta disponibilidade.

A adoção de recursos baseados em **inteligência artificial (IA) e aprendizado de máquina (ML)** será considerada diferencial relevante, especialmente para aprimoramento contínuo da acurácia dos

modelos, redução de falsos positivos e negativos (FAR/FRR), adaptação a novos vetores de fraude e melhoria da experiência do usuário durante o processo de autenticação.

Por fim, almeja-se uma solução que incorpore **boas práticas de usabilidade (UX), desempenho em tempo real e facilidade de integração**, assegurando sua aplicação eficiente, segura e transparente em diferentes jornadas digitais de autenticação, contribuindo para o fortalecimento da confiança e da segurança nos serviços públicos digitais.

2. Especificação do Objeto

2.1. Solução de Prova de Vivacidade (LIVENESS)

2.1.1. Dos Requisitos Funcionais da Solução

2.1.1.1. Prova de Vivacidade

2.1.1.1.1. A solução deve possuir detecção de vivacidade (detecção de vida) e deverá adotar tecnologia que assegure que a biometria foi capturada de um ser humano, impedindo a utilização de fotografias estáticas, máscaras, vídeos, imagens manipuladas, deepfake, emuladores, câmeras virtuais ou qualquer método que permita o uso de informação sem confirmação da vivacidade no momento da captura da informação biométrica;

2.1.1.1.2. A solução deve fazer a detecção de vivacidade de forma passiva, sem a necessidade de o usuário responder a uma prova (ex. piscar os olhos, mover o rosto ou qualquer outra exigência de movimento por parte do usuário);

2.1.1.1.3. A solução deve ser capaz de detectar quando o usuário estiver dormindo ou apresentar olhos fechados, garantindo que a validação biométrica somente prossiga mediante evidência de olhos abertos e estado ativo. Essa funcionalidade pode estar ativa ou inativa em critérios de configuração para atender necessidades de negócio ou para condições especiais em casos de pessoas enfermas e pessoas com deficiência.

2.1.1.1.4. Durante a etapa de captura, a solução deverá disponibilizar recursos de análise e aprovação da captura da face;

2.1.1.1.5. A solução de liveness deve ser capaz de realizar a confirmação da prova de vivacidade sob uma diversidade de condições de iluminação interiores e exteriores, favoráveis e adversas;

2.1.1.1.6. Caso a qualidade da imagem seja inadequada para validação, o verificador de qualidade da solução deverá informar que a imagem é insuficiente para o processo;

2.1.1.2. Detecção de Fraudes

2.1.1.2.1. A solução deve ser capaz de detectar os seguintes tipos de fraudes:

2.1.1.2.1.1. Quando ocorre a utilização máscara de papel 2D;

2.1.1.2.1.2. Quando ocorre a utilização de imagens impressas em papel;

2.1.1.2.1.3. Através de imagens digitais e vídeos (incluindo técnicas de deepfake) em telas de dispositivos móveis e monitores;

2.1.1.2.1.4. Através de imagens manipuladas por deepfake e quaisquer outras técnicas de manipulação de imagens;

2.1.1.2.1.5. Quando ocorre a utilização de máscara 3D em silicone, látex ou similares;

2.1.1.2.1.6. Quando ocorre a utilização de emuladores, câmeras virtuais, dispositivo root/jailbreak ou qualquer outro método que permita o uso de informação sem confirmação da vivacidade no momento da captura da informação biométrica;

2.1.1.3. Interoperabilidade e Integração

2.1.1.3.1. A solução de prova de vida deverá permitir a integração entre as soluções do Serpro que necessitem fazer esse tipo de validação. Esta camada de integração deverá ter as seguintes capacidades:

2.1.1.3.1.1. O componente deve capturar ao menos 03 (três) Imagens no formato JPG ou PNG com resolução de 720p HD (1280px x 720px);

2.1.1.3.1.2. O componente deve gerar um pacote criptografado e disponibilizar para a aplicação frontend, com no mínimo os seguintes dados: frames capturados, identificador único do dispositivo e identificador único da transação;

2.1.1.3.1.3. Qualquer comunicação do componente com o backend da solução, deve acontecer através de endpoints configurados no serviço do Serpro.

2.1.1.3.1.4. O componente deve permitir que a URL do endpoint referente à infraestrutura do Serpro seja configurável.

2.1.1.4. SDK, Componentes Frontend e Captura

2.1.1.4.1. A solução deve fornecer um componente frontend nas seguintes tecnologias: Android nativo e iOS nativa, web responsiva (com API integrável via javascript) e híbrida (flutter, cordova IOS e cordova Android) para a captura da face e verificação de enquadramento, tais componentes

deverão ser possíveis integrar-se com as aplicações do Serpro através de SDK (Software Development Kit);

2.1.1.4.2. A API do SDK Mobile deve possuir interface Java, Kotlin, Dart, Swift.

2.1.1.4.3. A solução deve disponibilizar callback de eventos durante a captura da imagem, ou seja, um mecanismo de executar código integrado ao SDK respondendo a eventos durante a prova de vida. Entre as ações que devem ser permitidas durante a captura de prova de vida estão:

2.1.1.4.3.1. Alternar câmera (frontal/traseira);

2.1.1.4.3.2. Acionar TTS (sintetizador de voz) ou execução de arquivo de áudio, em língua portuguesa, permitindo acessibilidade aos usuários.

2.1.1.4.3.3. Informar métricas de verificação de qualidade da imagem;

2.1.1.5. Resultado da Validação

2.1.1.5.1. Deve disponibilizar retorno com, minimamente, os resultados em cada validação:

2.1.1.5.1.1. Parecer da validação (aceita ou rejeitada);

2.1.1.5.1.2. Score ou percentual de vivacidade;

2.1.1.5.1.3. Score ou percentual de qualidade da imagem.

2.1.1.6. Identificação, Logs e Rastreabilidade da Transação

2.1.1.6.1. Deve ser possível identificar cada requisição de prova de vida por um identificador único da transação gerado pela solução, associando ainda cada requisição ao identificador único do dispositivo onde ela foi realizada.

2.1.1.6.1.1. Para cada requisição deve ser armazenado o momento da avaliação da prova de vida (timestamp) contendo data/hora/min/seg/milissegundo, assim como toda a informação associada ao processamento (logs), incluindo se ele foi realizado com sucesso e eventuais erros no cliente/SDK.

2.1.1.6.1.2. Em todos os casos, ainda deve ser registrado o resultado da avaliação da prova de vida contemplando scores de vivacidade e de qualidade de imagem e parecer final (aceita ou rejeitada), as imagens usadas para esta avaliação, assim como o que for necessário para reprodutibilidade, detalhada em item específico.

2.1.1.7. Armazenamento, Recuperação e Reprodutibilidade

2.1.1.7.1. Deve possibilitar o armazenamento e recuperação das imagens capturadas no processo de verificação de prova de vida, com a resolução original, de forma completa em formato jpeg ou png;

2.1.1.7.2. A solução deve armazenar e preservar as imagens e todas as informações necessárias para que seja possível repetir um procedimento de uma prova de vida (reprodutibilidade).

2.1.1.7.2.1. O ambiente de auditoria da solução deve fornecer as funcionalidades necessárias para a repetição do procedimento de prova de vida;

2.1.1.7.2.2. Estas informações devem ser preservadas para fins de auditoria em todas as avaliações e serão utilizadas para confirmar uma avaliação aceita ou uma suspeita de fraude identificada pela própria solução ou outras soluções do Serpro.

2.1.1.7.2.3. Tal funcionalidade deve estar disponível e será referenciada como “reavaliação de uma prova de vida”.

2.1.1.8. Bilhetagem

2.1.1.8.1. A solução deve fornecer uma funcionalidade de bilhetagem, de maneira que seja possível obter, por intervalo de horas, dias, meses e anos o total de provas de vidas realizadas, considerando critérios de parecer da prova de vida (aceita ou rejeitada) e totais.

2.1.1.8.2. Todas as informações produzidas nas consultas descritas no item anterior devem poder ser exportadas em relatórios padronizados;

2.1.1.8.3. A bilhetagem deve estar disponível a partir de um sistema Web e a partir de consultas automatizadas em uma API REST;

2.1.1.8.4. A quantidade de itens bilhetados corresponde ao número de provas de vidas concluídas. Essa quantidade precisa ser possível de validação com os registros de auditoria;

2.1.1.8.5. Deverão ser contabilizadas na bilhetagem as requisições de prova de vida concluídas, seja o resultado da verificação aceita ou rejeitada. Chamadas que não resultarem em uma detecção de prova de vida, ou seja, chamadas com erros ou quaisquer outros resultados não devem ser contabilizados.

2.1.1.9. Auditoria e Logs

2.1.1.9.1. Auditoria: os registros de prova de vida, com as imagens capturadas utilizadas associadas a eles e identificação de possível tentativa de fraude devem ser disponibilizadas em um sistema web, assim como via API REST documentada, com as seguintes características:

2.1.1.9.1.1. Controle de acesso definido pelo Serpro, permitindo o cadastro de usuários individuais e permissão de acesso definida apenas para esses usuários, através de solução própria ou integração com LDAP;

2.1.1.9.1.2. Todos os acessos a essa ferramenta devem ser gravados e posteriormente identificáveis, de maneira a permitir a rastreabilidade de eventuais vazamentos de dados sensíveis dos usuários;

2.1.1.9.1.3. Recuperação da imagem na qualidade (resolução) idêntica à capturada pelo dispositivo do usuário;

2.1.1.9.1.4. Informações detalhadas sobre a realização de cada prova de vida, incluindo momento da realização da prova de vida, identificação única da transação, parecer da validação (aceita ou rejeitada), score de vivacidade e score de qualidade da imagem, conforme campos especificados anteriormente;

2.1.1.9.1.5. Possibilidade de realizar consultas, buscas e filtros no ambiente web a partir do identificador único da transação, parecer da validação da prova de vida (aceita ou rejeitada), faixa temporal e faixa de valores dos indicadores e métricas gerados no processo;

2.1.1.9.1.6. Possibilidade de exportação dos dados produzidos em uma busca específica, considerando os filtros, contendo as imagens capturadas, para permitir análise de tentativas de fraude por parte de equipes do Serpro responsáveis por esta atividade;

2.1.1.9.1.7. Todas as consultas devem ter paginação;

2.1.1.9.1.8. Todas as consultas devem ter ordenação por qualquer campo, em ordem ascendente ou descendente;

2.1.1.9.1.9. O sistema de auditoria deve fornecer a funcionalidade de “reavaliação de prova de vida”, viabilizando a reprodutibilidade, com acesso controlado e registrado, conforme especificação descrita anteriormente. A critério do fabricante da solução pode haver tela específica para esta funcionalidade, localizando a tentativa de prova de vida a partir de seu identificador único da transação.

2.1.1.9.1.10. Disponibilizar API REST para recuperar as informações de prova de vida a partir do identificador único da transação;

2.1.1.9.1.11. Todos os eventos não previstos no funcionamento do componente frontend de prova de vida (por exemplo erros ou exceções) devem ser repassados ao aplicativo frontend integrado a este, de maneira a se possibilitar o tratamento adequado desses casos, para posterior gravação de log no backend.

2.1.1.10. APIs e Consulta aos Componentes

2.1.1.10.1. O volume de acessos deverá ser registrado e possível de ser consultado a partir de um mecanismo de bilhetagem, detalhado adiante em item específico;

2.1.1.10.2. Os registros completos das provas de vida deverão ser possíveis de serem consultados a partir de um sistema de auditoria e logs, detalhado adiante em item específico;

2.1.1.10.3. A solução deve fornecer mecanismos de consulta e interação com seus componentes (prova de vida, bilhetagem, auditoria e logs) através de APIs padronizadas e documentadas, com requisitos específicos também detalhados adiante em cada funcionalidade específica;

2.1.2. Dos Requisitos Não Funcionais

2.1.2.1. Conformidade, Certificação e Qualidade Técnica

2.1.2.1.1. A solução deve possuir carta de confirmação emitida por laboratórios credenciados pelo NIST/NVLAP ou FIDO Alliance para a sua aplicação de liveness. Os testes de detecção de vivacidade devem abranger os requisitos de Detecção de Ataque de Apresentação (Presentation Attack Detection – PAD), conforme a ISO/IEC 30107-3 e na modalidade de detecção de vivacidade passiva. Os laboratórios credenciados devem estar presentes nos endereços eletrônicos do FIDO Alliance <https://fidoalliance.org/certification/biometric-component-certification/fido-accredited-biometric-laboratories/> ou [https://www-nist.gov/niws/index.cfm?event=directory.detail&labId=690&programId=9&singleResult=true&csrFToken=AF384EDB-AFEE89AC61BDF8767E03773B4231E5B7](https://www.nist.gov/niws/index.cfm?event=directory.detail&labId=690&programId=9&singleResult=true&csrFToken=AF384EDB-AFEE89AC61BDF8767E03773B4231E5B7);

2.1.2.1.2. Deve garantir, minimamente, taxa de Attack Presentation Classification Error Rate (APCER) até 0,01% (zero virgula zero um por cento), através de autodeclaração do Fabricante da solução. A taxa poderá posteriormente, a critério do Serpro, ser aferida no processo de avaliação de amostra utilizando base interna do Serpro ou, por definição exclusiva do Serpro, através de uma base de validação disponibilizada pela Licitante;

2.1.2.1.3. Deve garantir, minimamente, taxa de Bona Fide Presentation Classification Error Rate (BPCER) até 5% (cinco por cento), através de autodeclaração do Fabricante da Solução. A taxa poderá posteriormente, a critério do Serpro, ser aferida no processo de homologação utilizando base interna do Serpro ou, por definição exclusiva do Serpro, através de uma base de validação disponibilizada pela Licitante;

2.1.2.1.4. A Contratada deverá viabilizar a validação indicada nos itens 2.1.2.1.2 e 2.1.2.1.3;

2.1.2.1.5. A solução deve ser capaz de manter as taxas de APCER e BPCER, dos itens 2.1.2.1.2 e 2.1.2.1.3, respectivamente, a partir de validações em amostras coletadas no ambiente de produção de uso típico da solução, a critério do Serpro.

2.1.2.2. Compatibilidade

2.1.2.2.1. Deve ser compatível com câmeras de dispositivos móveis, no mínimo: iOS versão 15 e Android versão 8, e evoluções posteriores;

2.1.2.2.2. Deve ser compatível com câmeras webcam, como também com os navegadores nas suas duas últimas versões mais recentes (versões desktop e mobile): Chrome, Firefox, Edge e Safari;

2.1.2.2.3. A captura da face pode ser realizada por câmera frontal e traseira de dispositivos móveis ou por webcam. A resolução mínima exigida para funcionamento da solução de prova de vida do Fabricante da Solução não pode ser superior a 2 (dois) megapixels;

2.1.2.3. Arquitetura, Implantação e Restrições Tecnológicas

2.1.2.3.1. A solução deve ser passível de utilização por multi-clientes (o Serpro e clientes do Serpro);

2.1.2.3.2. A arquitetura da solução deve ser baseada na execução da validação no servidor (backend) e fornecer componente, através de um Software Development Kit (SDK), para as funcionalidades que, porventura, forem realizadas pela aplicação (frontend).

2.1.2.3.3. A solução não poderá armazenar qualquer dado do sistema fora do ambiente sob gestão direta do Serpro;

2.1.2.3.4. Se houver armazenamento de arquivos deve seguir o padrão S3 (Simple Storage Service), e ser feito na infraestrutura de armazenamento de objeto do Serpro.

2.1.2.3.5. Se houver armazenamento de banco de dados, o software deve ser implantado na infraestrutura do Serpro e a Contratada deve fornecer a licença do software.

2.1.2.3.6. A solução deverá ser implantada no ambiente de nuvem privada do Serpro utilizando a infraestrutura de TI disponível na empresa, sem integração com serviços externos da contratada;

2.1.2.3.7. A infraestrutura deverá ser dimensionada e informada ao Serpro de forma a atender aos requisitos expostos;

2.1.2.3.8. A infraestrutura deverá ser dimensionada prevendo ambientes de desenvolvimento, homologação e produção;

2.1.2.3.9. A solução deverá ser implantada sobre plataforma comum de mercado, sem qualquer dependência ou presença de hardwares específicos;

2.1.2.3.10. A solução deverá ser capaz de ser executada em ambiente exclusivamente com CPU, e em ambiente com CPU e GPU. Deverá atender os requisitos de volumetria e throughput descritos neste documento.

2.1.2.3.11. Permitir execução em servidores Linux (Redhat ou Rocky/Alma Linux);

2.1.2.3.12. Permitir execução em plataforma baseada em contêineres docker.

2.1.2.3.13. A solução deverá permitir escalabilidade horizontal, ou seja, aumentar as instâncias da solução no cluster, permitindo a escalabilidade automática;

2.1.2.4. Segurança

2.1.2.4.1. A solução deve possuir mecanismos que impeçam qualquer tipo de quebra de segurança via força-bruta.

2.1.2.4.2. A Contratada deverá comunicar quaisquer vulnerabilidades encontradas na solução instalada no Serpro e ainda não solucionadas, bem como o prazo para disponibilização de rotina ou versão que solucione a falha detectada. Nos casos em que a vulnerabilidade permitir validações incorretas e/ou paralisação do ambiente, a Contratada deverá implementar medida de contorno para o restabelecimento do ambiente à condição operacional. A medida de contorno deverá ser substituída pela solução definitiva dentro de um prazo máximo de 30 (trinta) dias corridos;

2.1.2.4.3. No caso de identificação por parte do Serpro de uma avaliação da prova de vida ilegítima que produziu o parecer “aceito”, quando o esperado era “rejeitado”, levantadas as evidências de tal ocorrência, a Contratada deve fornecer solução paliativa em até 7 (sete) dias corridos e solução definitiva em até 30 (trinta) dias corridos.

2.1.2.4.3.1. A solução definitiva fornecida deve ser capaz de tratar qualquer caso similar ao identificado.

2.1.2.5. Monitoramento, Disponibilidade e Continuidade

2.1.2.5.1. O componente backend da solução deve possuir mecanismo de monitoramento ou telemetria, expondo via API o seu estado de funcionamento para garantir disponibilidade adequada.

2.1.2.5.1.1. A solução deve ser capaz de acionar serviços ou disponibilizar API de consulta de eventos para abrir Registros de Incidentes (RI), por exemplo em casos de erro ou indisponibilidade de módulos;

2.1.2.5.1.2. A solução deve fornecer um endpoint de monitoração para que seja possível verificar tempo de resposta e vazão da solução.

2.1.2.5.2. A infraestrutura deverá ser dimensionada prevendo uma taxa de disponibilidade de 99,5%, aferida de forma semanal, operando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

2.1.2.5.2.1. A infraestrutura deverá ser dimensionada prevendo ambiente redundante geograficamente, garantindo que caso um ambiente deixe de funcionar ou tenha degradação do tempo de resposta o segundo ambiente seja acionado para atendimento das requisições.

2.1.2.6. Desempenho, Volumetria e Throughput

2.1.2.6.1. A solução deve atender às seguintes necessidades de tempo de resposta, volumetria, throughput e acessos abaixo definidas:

2.1.2.6.1.1. Atender em torno de 60.000.000 (sessenta milhões) de transações mensais;

2.1.2.6.1.2. Responder com sucesso 100 (cem) transações/seg;

2.1.2.6.1.3. Consultas aos logs de auditoria, de uma paginação de pelo menos 10 (dez) registros, devem ser concluídas em até 5s;

2.1.2.6.1.4. Exportações dos logs de auditoria, incluindo as imagens consideradas nas requisições, até uma quantidade de 200 requisições, devem ser concluídas em até 1 (um) minuto;

2.1.2.6.1.5. Consulta ao bilhetador e geração de relatório consolidado, relacionadas a qualquer intervalo de datas, devem ser concluídas em até 1 (um) minuto.

2.1.2.6.2. Deve possuir o tempo de detecção de liveness de máximo 5 (cinco) segundos.

2.1.2.7. Matriz de Compatibilidade

2.1.2.7.1. A solução proposta deve manter compatibilidade com os seguintes ambientes de software, que serão instalados on-premise no Serpro;

2.1.2.7.1.1. VMWare 6.5 ou versão superior;

2.1.2.7.1.2. Red Hat ou Rocky/Alma Linux - versões mais atuais;

2.1.2.7.1.3. Manter compatibilidade com os seguintes ambientes de hardware:

2.1.2.7.1.3.1. Processador INTEL-Based;

2.1.2.7.1.3.2. Processador AMD-Based;

2.1.2.7.1.4. A Solução deve operar e ser compatível com ambientes operando em Fabrics;

2.1.2.7.1.5. SAN (Storage Area Network), baseados em protocolo FC (Fibre Channel);

2.1.2.7.1.6. A Solução deve operar e ser compatível com protocolos para armazenamento de objetos: HTTP/HTTPS-RestAPI, S3 e SWIFT;

2.1.2.7.1.7. A Solução deve ser compatível com o protocolo de rede TCP/IP, nas versões IPv4 e IPv6;

2.1.2.7.1.8. A Solução deverá ser capaz de interoperar em ambientes com NAT (Network Address Translation) e Firewalls;

2.1.2.7.1.9. A Solução deve obrigatoriamente operar e ser compatível com ambiente virtualizado;

2.1.2.7.1.10. A Solução deve operar e ser compatível com ambientes clusterizados;

2.1.2.7.1.11. Permitir execução em plataforma baseada em contêineres docker.

2.1.2.7.1.12. Caso sejam necessários programas clientes desktop para desenvolvimento e administração da aplicação, estes deverão ser compatíveis, no mínimo, com a plataforma de software livre Ubuntu 22.04 e versão superior ou com a plataforma Windows 10 e versão superior;

2.1.2.7.1.13. O sistema deve rodar em plataforma 32 e/ou 64 bits.

2.1.2.8. Documentação

2.1.2.8.1. A solução deve possuir documentação completa e atualizada em língua portuguesa que contemple sua instalação, manutenção, utilização e atualização.