



TRIBUNAL REGIONAL ELEITORAL DE SERGIPE
Capucho - Bairro CENAF, Lote 7, Variante 2 - CEP 49081-000 - Aracaju - SE - <http://www.tre-se.jus.br>

ESTUDOS TÉCNICOS PRELIMINARES DE STIC

HISTÓRICO DE VERSÕES

IDENTIFICAÇÃO DA VERSÃO DO SEI	DATA DA VERSÃO	RESPONSÁVEL	ALTERAÇÕES (indicar tópicos alterados)	OBSERVAÇÕES (se couber)
DOC SEI 1754696	17/09/2025	Integrantes Demandante e Técnico	1ª versão	Sem observações
DOC SEI 1774511	04/11/2025	Integrantes Demandante e Técnico	2ª versão	Sem observações
DOC SEI 1780217	28/11/2025	Integrantes Demandante e Técnico	3ª versão	Ajustes feitos após diligências da assessoria jurídica.
DOC SEI 1788340	09/12/2025	Integrantes Demandante e Técnico	4ª versão	Ajustes após parecer da assessoria jurídica.

I. DADOS DO PROCESSO

1.1 Processo administrativo SEI nº 0006368-08.2025.6.25.8000

1.2 Objeto: Contratação de Plataforma de Gestão do Ciclo de Vida de Desenvolvimento de Software (DevOps/ALM – Application Lifecycle Management).

1.3 Unidade(s) Demandante(s) (se houver): Coordenadoria de Sistemas Corporativos (COSIS)	
1.4 Unidade Solicitante	
Responsável titular - Jeirlan Correia Palmeira ou susbtituta(o) automática(o)/designada(o).	Unidade: COSIS/STI
1.5 Unidade Técnica (se houver)	
1.6 Equipe de Planejamento da Contratação (se houver)	
Integrante Demandante: Titular - Fernando de Souza Lima Substituto - Martha Coutinho de Faria Alves	Unidade: NAC/STI NAI/STI
Integrante Técnico (se houver): Titular - Diego Medeiros Vilar Oliveira Substituto - Jeirlan Correia Palmeira	Unidade: SESEL/STI COSIS/STI
Integrante Administrativo (se houver): Titular - Ricardo Loeser de Carvalho Filho Substituto - Valéria Maria dos Santos	Unidade: ASPLAN/SAO ASPLAN/SAO
1.7 Responsável pela Aprovação do Estudo Preliminar:	
N o m e : Rubens Lisbôa Maciel Filho ou susbtituta(o) automática(o)/designada(o).	Unidade: DG
1.8 Fiscais Previamente Indicados (opcional):	
Fiscal Técnico: Titular - Fernando de Souza Lima Substituto - Cosme Rodrigues de Souza	Unidade: NAC/STI COINF/STI
Fiscal Administrativo: Titular - Ricardo Loeser de Carvalho Filho Substituto - Valéria Maria dos Santos	Unidade: ASPLAN/SAO ASPLAN/SAO
Fiscal Setorial: Não se aplica.	Unidade: Não se aplica.

Gestão da Contratação: Titular - Fernando de Souza Lima Substituto - Cosme Rodrigues de Souza	Unidade: NAC/STI COINF/STI
---	----------------------------------

SUMÁRIO

1. Capítulo 1: Análise de viabilidade da contratação

- 1.1 Contextualização
- 1.2 Identificação da demanda no Plano de Contratações de STIC
 - 1.2.1
 - 1.2.2 Alinhamento da solução
- 1.3 Caracterização da demanda
 - 1.3.1 Definição e especificação das necessidades
 - 1.3.2 Definição e especificação de requisitos
 - 1.3.3 Requisitos funcionais
 - 1.3.4 Aderência a padrões e modelos
- 1.4 Atendimento da demanda
 - 1.4.1 Portal do Software Público Brasileiro
 - 1.4.2 Soluções de TIC
 - 1.4.3 Contratações públicas similares
 - 1.4.4 Soluções similares em outros órgãos
 - 1.4.5 Modelos de aquisição/prestação do serviço
 - 1.4.6 Capacidade e alternativas do mercado de TIC
 - 1.4.7 Contratações correlatas e/ou interdependentes
- 1.5 Análise dos custos totais da demanda
- 1.6 Escolha e justificativa da solução
 - 1.6.1 Descrição da solução escolhida
 - 1.6.2 Benefícios esperados
 - 1.6.3 Resultados esperados
 - 1.6.4 Relação entre a demanda prevista e a quantidade de bens e/ou serviços contratados
- 1.7 Declaração de viabilidade da contratação

2. Capítulo 2: Sustentação do contrato

- 2.1 Adequação do ambiente
- 2.2 Recursos materiais e humanos
- 2.3 Continuidade do fornecimento
- 2.4 Transição contratual e encerramento do contrato
- 2.5 Estratégia de independência tecnológica

3. Capítulo 3: Estratégia para a contratação

4. Capítulo 4: Análise de riscos

4.1 Riscos mapeados

5. Aprovação e assinatura

6. Ciência da instância deliberativa de TIC

7. Anexos

Anexo A – Lista de potenciais fornecedores

Anexo B – Propostas comerciais

Anexo C – Contratações públicas similares

1. CAPÍTULO 1: ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1.1 CONTEXTUALIZAÇÃO

1.1.1.1 O TRE-SE utiliza atualmente o GitLab, em sua versão gratuita, como plataforma principal para a gestão do desenvolvimento de software. A ferramenta é amplamente reconhecida no mercado por integrar, em um único ambiente, funcionalidades de controle de versões, gestão de projetos, automação de processos, integração e entrega contínua (CI/CD), além de recursos essenciais do ciclo de vida do desenvolvimento.

1.1.2 Justificativa da Adoção Inicial

1.1.2.1 A escolha pela plataforma ocorreu porque, à época, nenhuma outra solução disponível no mercado apresentava maturidade ou alinhamentos técnicos suficientes para atender às necessidades institucionais do TRE-SE. As alternativas existentes eram incipientes ou não contemplavam plenamente os requisitos demandados pelo Tribunal.

1.1.2.2 Durante o processo de avaliação inicial, em 2018, foram analisados fatores determinantes, tais como:

- Maturidade tecnocientífica da solução;
- Custos indiretos de adaptação e eventual migração;
- Limitações de suporte e conformidade das alternativas concorrentes;
- Aderência da plataforma aos fluxos de trabalho já consolidados.

1.1.2.3 Esses elementos reforçaram a escolha do GitLab como solução-base, que se consolidou como a espinha dorsal dos processos internos, fundamentada em padrões abertos e plenamente integrada às rotinas de desenvolvimento.

1.1.3 Evolução das Necessidades Institucionais

1.1.3.1 Com o decorrer dos anos, as demandas do Tribunal tornaram-se mais complexas,

exigindo funcionalidades avançadas que **não estão presentes na edição gratuita** da ferramenta. Entre os recursos necessários destacam-se:

- Funcionalidades aprimoradas de segurança;
- Mecanismos de governança corporativa;
- Auditoria e trilhas de conformidade;
- Recursos de escalabilidade;
- Monitoramento avançado;
- Automações críticas de processos.

1.1.3.2 Tais capacidades são indispensáveis para a continuidade e maturidade do ciclo de desenvolvimento em um ambiente institucional complexo.

1.1.4 Necessidade de Evolução da Solução

1.1.4.1 Considerando o aumento da complexidade operacional e a necessidade de aderência às práticas avançadas de governança de TI, torna-se imprescindível buscar uma solução que atenda plenamente aos requisitos institucionais.

1.1.4.2 A adoção de uma plataforma mais completa representa:

- Uma evolução natural da capacidade institucional;
- Alinhamento às normas e melhores práticas de governança;
- Preservação dos investimentos realizados em processos, infraestrutura e capacitação;
- Redução dos riscos de dependência tecnológica crítica;
- Fortalecimento da segurança, da continuidade operacional e da transparência.

1.1.5 Considerações finais

1.1.5.1 A adoção de uma solução mais completa representa uma evolução natural e alinhada às normas e às melhores práticas de governança, preservando a soberania tecnológica e garantindo a proteção dos investimentos realizados em processos e infraestrutura. Essa medida contribui para a mitigação de riscos relevantes e fortalece a continuidade operacional, a transparência e a segurança institucional.

1.2 IDENTIFICAÇÃO DA DEMANDA NO PLANO DE CONTRATAÇÕES DE STIC

1.2.1 A presente demanda está registrada no Plano de Contratações de Soluções de Tecnologia da Informação e Comunicação (STIC) do TRE/SE, vinculada à Ação Orçamentária **33.90.40.06.0006 – Locação de Softwares**, sob responsabilidade da unidade demandante **STI/COSIS**, conforme anexo I - versão 2 (doc. 1744404) da Portaria nº 4, de 9 de dezembro de 2024, que dispõe sobre a aprovação do plano de Contratações Anual para o exercício de 2025.

1.2.2 ALINHAMENTO DA SOLUÇÃO

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
OE-8	Entregar soluções de TIC que satisfaçam as necessidades a um custo aceitável.

Tabela 1 – Alinhamento aos Objetivos Estratégicos. Fonte: Anexo da Portaria Normativa TRE-SE

ALINHAMENTO AO PDTIC - 2025-2026			
ID	ENTIC-JUD	Justiça Eleitoral de Sergipe	Secretaria de Tecnologia da Informação e Comunicação
OE-8	Promover Serviços de Infraestrutura e Soluções Corporativas	Agilidade e Produtividade na Prestação Jurisdicional	Entregar soluções de TIC que satisfaçam as necessidades, a um custo aceitável.

Tabela 2 – Alinhamento ao Plano Diretor de TIC. Fonte: Anexo da Portaria Normativa TRE-SE nº 22/2025 (1667427).

1.3 CARACTERIZAÇÃO DA DEMANDA

1.3.1 DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES

- 1.3.1.1 Permitir que múltiplas equipes trabalhem de forma integrada e simultânea, sem restrições de acesso;
- 1.3.1.2 Possibilitar automação completa de testes, builds e deploys, garantindo eficiência e confiabilidade;
- 1.3.1.3 Assegurar controle de permissões, auditoria, histórico de alterações e conformidade com normas de governança de TI;
- 1.3.1.4 Oferecer dashboards, relatórios e funcionalidades de monitoramento que permitam transparência e controle efetivo sobre todas as fases do desenvolvimento.

1.3.2 DEFINIÇÃO E ESPECIFICAÇÃO DE REQUISITOS

1.3.3 REQUISITOS FUNCIONAIS

- 1.3.3.1 Requisitos de arquitetura tecnológica (configuração)
 - 1.3.3.1.1 Os requisitos estão dispostos no anexo “Especificações Técnicas”.
- 1.3.3.2 Requisitos de capacitação
 - 1.3.3.2.1 Não serão exigidos requisitos de capacitação para a presente contratação.
- 1.3.3.3 Requisitos de manutenção
 - 1.3.3.3.1 A solução a ser contratada deverá atender aos seguintes requisitos de manutenção, de modo a garantir a continuidade operacional, a confiabilidade e a segurança dos serviços:
 - a) **Atualizações e Correções:** Disponibilização contínua de atualizações corretivas, evolutivas e de segurança, sem impacto na integridade dos dados ou indisponibilidade prolongada da solução;
 - b) **Alta Disponibilidade:** Garantia de disponibilidade mínima, com mecanismos de redundância e recuperação em caso de falhas;

- c) **Escalabilidade e Sustentação:** Capacidade de manutenção da solução de forma escalável, permitindo ampliação de usuários, projetos e integrações sem comprometer o desempenho;
- d) **Monitoramento e Relatórios:** Disponibilização de ferramentas de monitoramento de desempenho e geração de relatórios técnicos de funcionamento, atualizações aplicadas e incidentes registrados;
- e) **Continuidade Operacional:** Procedimentos documentados de contingência e recuperação de desastres, garantindo a retomada das atividades em prazos adequados em caso de falha crítica;
- f) **Compatibilidade e Integração:** Manutenção da compatibilidade com sistemas operacionais, navegadores e ferramentas de integração mais utilizados, evitando obsolescência precoce.

1.3.3.4 Requisitos de projeto e de implementação

1.3.3.4.1 Não serão exigidos requisitos de projeto e implementação para a presente contratação.

1.3.3.5 Requisitos de implantação

1.3.3.5.1 Não serão exigidos requisitos de implantação para a presente contratação.

1.3.3.6 Requisitos de experiência profissional

1.3.3.6.1 Não serão exigidos requisitos de experiência profissional para a presente contratação.

1.3.3.7 Requisitos de formação da equipe

1.3.3.7.1 Não serão exigidos requisitos de formação da equipe para a presente contratação.

1.3.3.8 Requisitos temporais

1.3.3.8.1 O prazo de entrega é de **15 (quinze) dias**, contados da assinatura do Contrato ou do recebimento da Nota de Empenho, conforme o caso.

1.3.3.8.1.1 A(O) CONTRATADA(O) deve estar atenta aos demais prazos estabelecidos nos instrumentos da contratação.

1.3.3.9 Requisitos de segurança e privacidade

1.3.3.9.1 A(O) CONTRATADA(O) deverá manter sigilo acerca de informações do ambiente do CONTRATANTE que eventualmente venha a ter acesso em decorrência da execução da contratação, sob pena de responsabilidade cível, penal e administrativa:

- a) Sobre todas as informações relativas à prestação dos serviços, incluindo documentação, procedimentos, configurações de equipamentos, softwares, políticas e quaisquer informações obtidas pela(o) CONTRATADA(O) em função da prestação dos serviços;
- b) Sobre a política de segurança adotada pelo CONTRATANTE e as configurações de hardware e de softwares decorrentes;
- c) Sobre o processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;
- d) Sobre o processo de implementação, no ambiente do CONTRATANTE, dos mecanismos de criptografia e de autenticação.

1.3.3.9.2 A(O) CONTRATADA(O) não poderá efetuar, sob qualquer pretexto, a transferência de qualquer responsabilidade que lhe compete para outras entidades, sejam fabricantes, técnica(o)s, subempreiteira(o)s etc, sem a anuência expressa do CONTRATANTE.

1.3.3.9.3 A(O) CONTRATADA(O) deverá, ainda, submeter suas(seus) profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências.

1.3.3.10 Requisitos sociais, ambientais e culturais

1.3.3.10.1 Requisitos sociais

a) Os prestadores de serviço que acessarem a infraestrutura devem seguir normas de conduta e confidencialidade, evitando uso indevido de informações.

1.3.3.10.2 Requisitos ambientais

a) Não se aplica.

1.3.3.10.3 Requisitos culturais

a) Os prestadores devem adaptar sua atuação às normas internas do órgão, respeitando hierarquias, fluxos de aprovação e boas práticas de segurança da informação.

1.3.3.11 Requisitos legais

1.3.3.11.1 O presente processo de contratação deve estar aderente à Constituição Federal, à Lei 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Resolução CNJ 468, de 15 de julho de 2022 (Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça) e a outras legislações aplicáveis, tais como:

a) Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte;

b) Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados);

c) Decreto nº 7.174, de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

d) Instrução Normativa SLTI/MP nº 01, de 19 de Janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional;

e) Instrução Normativa (IN) SGD/ME nº 94, de 23 de dezembro de 2022: normas para Contratação de Soluções de TIC pelos órgãos integrantes do SISP;

f) Lei 8.078, 11 de setembro de 1990 (Código de Defesa do Consumidor);

g) Resolução TSE nº 23.644/2021 — Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

h) Resolução TRE-SE nº 10/2019 – Dispõe sobre a Política de Segurança da Informação (PSI) da Justiça Eleitoral de Sergipe;

i) Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 - Estabelece modelo de contratação de software e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

1.3.3.12 Demais requisitos aplicáveis

1.3.3.12.1 Não se aplica.

1.3.4 ADERÊNCIA A PADRÕES E MODELOS

1.3.4.1 *Modelo Nacional de Interoperabilidade – MNI*

1.3.4.1.1 A Plataforma de Gestão do Ciclo de Vida de Desenvolvimento de Software a ser contratada deverá atender aos padrões do Modelo Nacional de Interoperabilidade (MNI), garantindo:

- a) **Interoperabilidade** com outros sistemas governamentais;
- b) **Segurança e integridade da informação**, conforme diretrizes do MNI;
- c) **Capacidade de integração futura** via APIs ou outros mecanismos padronizados;
- d) **Documentação comprobatória de conformidade**, permitindo auditoria e verificação pelo órgão contratante.

1.3.4.2 *Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil*

1.3.4.2.1 A Plataforma de Gestão do Ciclo de Vida de Desenvolvimento de Software a ser contratada deverá estar em conformidade com a **Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)**, garantindo:

- a) **Autenticação e identificação segura de usuários** por meio de certificados digitais válidos pela ICP-Brasil;
- b) **Assinatura digital de documentos e artefatos** gerados ou gerenciados pelo sistema, com validade jurídica;
- c) **Criptografia de dados** conforme padrões da ICP-Brasil para proteção da integridade e confidencialidade da informação;
- d) **Documentação comprobatória de conformidade** com os padrões ICP-Brasil, permitindo auditoria e verificação pelo órgão contratante.

1.3.4.3 *Modelo de Requisitos MoReq-Jus*

1.3.4.3.1 O sistema GitLab a ser contratado deverá atender aos princípios do **Modelo de Requisitos para Gestão Eletrônica de Documentos e Processos (MoReq-Jus)**, garantindo:

- a) **Organização e classificação de documentos e processos** segundo padrões reconhecidos;
- b) **Gestão eletrônica de registros e metadados** compatível com MoReq-Jus;
- c) **Controle de versão, rastreabilidade e auditoria** dos artefatos e documentos armazenados;
- d) **Documentação comprobatória de conformidade** com MoReq-Jus, permitindo verificação e auditoria pelo órgão contratante.

1.4 ATENDIMENTO DA DEMANDA

1.4.1 PORTAL DO SOFTWARE PÚBLICO BRASILEIRO

1.4.1.1 Não se aplica.

1.4.2 SOLUÇÕES DE TIC

1.4.2.1 Preâmbulo

1.4.2.1.1 A necessidade consiste na contratação de uma **plataforma Git completa**, para implantação **on-premise** (sem utilização de nuvem pública), que ofereça **suporte integral aos fluxos DevSecOps adotados pela instituição** e seja **compatível com ambientes Linux**.

1.4.2.1.2 A solução deverá contemplar, no mínimo, os seguintes requisitos:

- Controle de versão Git com suporte a **pull/merge requests** e mecanismos de aprovação;
- Possibilidade de definição de **responsáveis (“ownership”) por arquivos e diretórios**;
- Execução de **pipelines de CI/CD**, tanto acionados manualmente quanto por gatilhos automáticos;
- **Repositório de artefatos**, apto a armazenar binários, pacotes e demais artefatos gerados no ciclo de desenvolvimento;
- **Registro de imagens Docker** e repositórios de pacotes (como npm, Maven, entre outros);
- Funcionalidades avançadas de **segurança de código**, incluindo:
 - SAST (análise estática de código-fonte),
 - DAST (análise dinâmica),
 - inspeção e verificação de dependências,
 - detecção e correção orientada a vulnerabilidades.

1.4.2.1.3 A plataforma deve ainda disponibilizar **dashboards gráficos para monitoramento, auditoria e gestão de riscos**, permitindo a visualização centralizada de vulnerabilidades, conformidade, evolução da saúde dos projetos e trilhas de auditoria, assegurando rastreabilidade end-to-end do ciclo de desenvolvimento.

1.4.2.2 Solução 1: Migração para outra plataforma gratuita de DevOps com melhor suporte a padrões

1.4.2.2.1 Fundamentação

a) Avaliar alternativas gratuitas que ofereçam maior conformidade com padrões governamentais.

1.4.2.2.2 Benefícios

- a) Possível maior aderência a padrões e diretrizes de conformidade;
- b) Ausência de custo de licenciamento.

1.4.2.2.3 Desvantagens:

- a) Necessidade de migração de repositórios e pipelines existentes;
- b) Treinamento da equipe para adaptação à nova plataforma;
- c) Possíveis limitações em recursos avançados de DevOps.
- d) Custo excessivo de horas trabalhadas.

1.4.2.3 Solução 2: Migração para uma versão comercial da plataforma atualmente utilizada (GitLab)

1.4.2.3.1 Fundamentação

a) Contratação da versão paga, que oferece recursos avançados de DevOps, segurança, compliance e suporte técnico.

1.4.2.3.2 Benefícios

- a) Recursos avançados de CI/CD;
- b) Conformidade com padrões de segurança e auditoria;
- c) Suporte técnico oficial;
- d) Controle detalhado de permissões e grupos;
- e) Integração com sistemas internos e conformidade com padrões governamentais, como MNI e ICP-Brasil.

1.4.2.3.3 Desvantagens

- a) Custo de licenciamento;

1.4.2.4 Solução 3: Migração para outra plataforma de DevOps

1.4.2.4.1 Fundamentação

a) Consiste na adoção de plataformas concorrentes ao GitLab que ofereçam funcionalidades equivalentes, com melhor suporte a padrões governamentais.

1.4.2.4.2 Benefícios

- a) Maior aderência a padrões e requisitos de compliance;
- b) Recursos avançados de CI/CD e integração com ferramentas externas;
- c) Suporte técnico oficial ou apoio de comunidade ativa, dependendo da plataforma escolhida;

1.4.2.4.3 Desvantagens

- a) Necessidade de migração de repositórios e pipelines já existentes;
- b) Treinamento da equipe para adaptação à nova solução;
- c) Eventuais restrições de integração com sistemas internos ou legados, dependendo da plataforma selecionada.
- d) Custo de migração.

1.4.2.5 Análise comparativa das soluções

1.4.2.5.1 Solução 1: Migração para outra plataforma gratuita de DevOps com melhor suporte a padrões

1.4.2.5.1.1 Apesar de apresentar custo de licenciamento nulo, a migração para outra plataforma gratuita de DevOps não se mostra viável para o órgão, em razão dos seguintes fatores:

- a) O GitLab, mesmo em sua versão gratuita, é uma solução madura, amplamente utilizada e reconhecida no mercado;
- b) O processo de migração de repositórios, pipelines e integrações existentes implicaria custos indiretos elevados, tanto em horas de trabalho especializadas quanto em treinamento da equipe, neutralizando a economia aparente;
- c) As alternativas gratuitas carecem de suporte técnico oficial, dependendo exclusivamente de comunidades voluntárias, o que representa risco elevado para a continuidade e estabilidade das operações do órgão;
- d) A troca de plataforma pode gerar incompatibilidades técnicas, despadronização de processos

e impacto negativo na produtividade da equipe, em virtude da necessidade de adaptação a novos fluxos e ferramentas;

1.4.2.5.1.2 Diante desses aspectos, conclui-se que a Solução 1 não atende às necessidades do órgão, apresentando riscos que superam os eventuais benefícios.

1.4.2.5.2 Solução 2: Migração para versão comercial da plataforma atualmente utilizada (GitLab)

1.4.2.5.2.1 A adoção de uma versão comercial da solução já utilizada pelo órgão (GitLab) demonstra-se aderente às necessidades identificadas para implantação de uma plataforma Git completa, on-premise, com suporte integral aos fluxos DevSecOps. Essa alternativa atende aos requisitos funcionais, operacionais e de segurança descritos no presente documento, destacando-se pelos seguintes aspectos:

a) Continuidade operacional – Aproveita a infraestrutura existente, evitando riscos e custos de transição para uma nova plataforma e garantindo a preservação dos processos e repositórios já consolidados.

b) Atendimento pleno às funcionalidades essenciais, incluindo:

- controle de versão com pull/merge requests e mecanismos de aprovação;
- definição de responsáveis (“ownership”) por diretórios e arquivos;
- pipelines de CI/CD acionados manualmente ou por gatilhos automáticos;
- repositório de artefatos, registro Docker e repositórios de pacotes (npm, Maven, etc.).

c) Recursos avançados de DevSecOps, com suporte nativo às práticas de segurança de código, como:

- SAST (análise estática),
- DAST (análise dinâmica),
- inspeção automática de dependências,
- detecção, correção e acompanhamento de vulnerabilidades ao longo do ciclo de desenvolvimento.

d) Disponibilização de dashboards de governança e auditoria, permitindo monitoramento centralizado de riscos, vulnerabilidades, conformidade e evolução da saúde dos projetos, assegurando rastreabilidade completa end-to-end.

e) Suporte técnico oficial, com níveis de serviço definidos (SLA), reduzindo riscos operacionais e aumentando previsibilidade e confiabilidade da operação.

f) Escalabilidade na gestão de usuários, grupos e permissões, característica fundamental para ambientes institucionais de grande porte.

g) Integração corporativa aprimorada, com suporte a diretórios LDAP/AD, protocolos de autenticação e ferramentas internas de monitoramento e gestão.

h) Evolução tecnológica contínua, garantida pelo fornecedor, permitindo acompanhamento das melhores práticas e tendências de mercado.

1.4.2.5.2.2 Diante do exposto, a Solução 2 consolida-se como alternativa robusta, sustentável e aderente às necessidades institucionais, equilibrando custo-benefício, maturidade tecnológica, segurança, escalabilidade e conformidade com padrões governamentais e boas práticas de desenvolvimento seguro.

1.4.2.5.3 Solução 3: Migração para outra plataforma de DevOps

1.4.2.5.3.1 Dentre as plataformas amplamente consolidadas no mercado para operação self-hosted (on-premise), considerando requisitos de governança, segurança, rastreabilidade, integração corporativa e aderência a fluxos DevSecOps, destacam-se as seguintes:

1. Atlassian Bitbucket Data Center

1.1 Solução corporativa self-hosted para controle de versão Git, com integração nativa ao ecossistema Atlassian (Jira, Confluence, entre outros). Entretanto:

- **Pipeline de CI/CD:** a plataforma não dispõe de pipeline nativo integrado. A automação de builds geralmente requer o uso do **Bamboo** (solução de CI on-premise da Atlassian) ou ferramentas externas, como **Jenkins**;
- **Segurança (SAST/DAST):** não oferece mecanismos próprios de varredura de segurança. A análise de código depende de soluções externas, com visualização dos resultados por meio do recurso **Code Insights**;
- **Gerenciamento de artefatos:** o registro e gestão de pacotes e imagens de contêiner dependem de soluções complementares, como **Nexus** ou **Artifactory**.

1.2 Dessa forma, embora a solução seja consistente na gestão de código e bem integrada às ferramentas Atlassian, o **Bitbucket Data Center** exige a construção de uma cadeia adicional de produtos para viabilizar um ciclo completo de DevSecOps.

1.3 Além disso, a Atlassian anunciou em 08/09/2025 que seus produtos on-premise (família Atlassian Data Center) serão **descontinuados**:
<https://www.atlassian.com/blog/announcements/atlassian-ascend>.

2. Azure DevOps Server (on-premise)

2.1 Solução corporativa da Microsoft que oferece:

- Repositórios Git integrados;
- Pipelines de CI/CD (Azure Pipelines);
- Gerenciamento de pacotes para artefatos e dependências (Azure Artifacts).

2.2 Todavia:

- A versão Server (on-premise) segue suportada oficialmente para execução em ambiente Windows, o que limita sua adoção em instituições baseadas majoritariamente em Linux;
- Não possui mecanismos nativos integrados para SAST/DAST, dependendo da integração com ferramentas de terceiros, como SonarQube, Veracode, Checkmarx, entre outras.

2.3 Dessa forma, ainda que ofereça boa integração funcional para desenvolvimento interno, não atende completamente ao ciclo DevSecOps sem a adição de ferramentas complementares de segurança.

3 GitHub Enterprise Server (self-hosted)

3.1 O GitHub Enterprise Server é a edição corporativa para execução on-premise, garantindo controle institucional sobre dados e conformidade. Entre suas funcionalidades:

- Gestão completa de repositórios Git, com pull requests, revisão de código, controle de permissões e workflows;

- Disponibiliza GitHub Actions executados localmente, permitindo pipelines de CI/CD totalmente internos;
- Integração com diretórios corporativos como LDAP e Active Directory;
- Oferece recursos de segurança como gestão de dependências vulneráveis e análise de exposições, além de integração com ferramentas de mercado.

3.2 No entanto:

- A análise avançada de segurança, como SAST via CodeQL e funcionalidades ampliadas de governança e compliance, depende de módulos adicionais de licenciamento (antes reunidos em Advanced Security, agora segmentados em Code Security e Secret Protection);
- A operação pode demandar infraestrutura especializada (appliances virtuais e GitHub runners) e apresenta menor flexibilidade de personalização do ambiente operacional quando comparada a soluções mais abertas.

3.3 Em síntese, o GitHub Enterprise Server é maduro para desenvolvimento e automação em ambiente corporativo, porém parte de suas capacidades avançadas de segurança depende de licenciamento e configuração adicionais.

4. Outras soluções (Gitea, Gogs, Phabricator e similares)

4.1 São plataformas de baixo custo e menor complexidade operacional, porém:

- Não oferecem CI/CD nativo;
- Não possuem mecanismos integrados de SAST/DAST;
- Dependem amplamente de integrações externas para evoluir além do controle básico de código.

4.2 Por esse motivo, embora adequadas para ambientes pequenos ou com baixa exigência de governança, não atendem aos requisitos institucionais de segurança, rastreabilidade, auditoria, continuidade e operação em escala.

1.4.2.6 Conclusão

1.4.2.6.1 Diante da avaliação técnica realizada, verifica-se que as alternativas disponíveis no mercado, quando operadas em ambiente on-premise, exigem combinações heterogêneas de ferramentas e fornecedores para viabilizar o ciclo completo de desenvolvimento, automação, segurança, rastreabilidade e governança. Essa fragmentação tecnológica tende a elevar custos operacionais e de licenciamento, aumentar a complexidade de integração, demandar maior esforço de suporte contínuo e introduzir riscos adicionais decorrentes da dependência de múltiplos sistemas, cada qual com sua própria evolução, ciclo de atualização e modelo de suporte.

1.4.2.6.2 A análise das alternativas disponíveis evidencia que a maior parte das soluções self-hosted requer a integração de diversas ferramentas de diferentes fornecedores para compor o ciclo completo de desenvolvimento — incluindo versionamento de código, pipelines de CI/CD, armazenamento de artefatos, varredura de vulnerabilidades (SAST/DAST) e mecanismos de auditoria e governança. Esse cenário fragmentado tende a elevar custos operacionais e de licenciamento, aumentar a dependência de múltiplas tecnologias, ampliar o esforço de suporte e manutenção e criar uma superfície maior de falhas decorrentes da integração entre produtos heterogêneos.

1.4.2.6.3 Adicionalmente, a adoção de plataformas distintas daquela atualmente utilizada pelo órgão implica riscos de migração significativos, tais como:

- necessidade de transferir repositórios, pipelines, integrações e histórico técnico para uma nova solução, com possibilidade de perda de metadados, configurações e trilhas de auditoria;
- interrupções temporárias ou redução de produtividade durante o período de transição;
- retrabalho para reescrever pipelines, reconfigurar credenciais, redesenhar integrações e validar mecanismos de segurança;
- necessidade de treinamento intensivo das equipes para adaptação a novas interfaces, terminologias e modelos operacionais;
- risco de incompatibilidades com sistemas internos legados, o que pode demandar desenvolvimento adicional, novos componentes intermediários ou ajustes complexos de arquitetura.

1.4.2.6.4 Esses fatores, somados, tornam a substituição da plataforma atual um processo custoso, de elevada complexidade e com potencial impacto operacional.

1.4.2.6.5 A solução atualmente utilizada pelo órgão, o GitLab, em sua versão comercial, apresenta-se como a plataforma capaz de atender integralmente aos requisitos levantados de forma nativa, unificada e já consolidada na operação institucional. Além de preservar os investimentos e fluxos já estabelecidos, a adoção da versão paga do GitLab oferece maturidade técnica, aderência plena às práticas DevSecOps, suporte oficial, evolução tecnológica garantida, maior previsibilidade operacional e redução significativa da complexidade administrativa, ao concentrar em uma única solução todos os elementos do ciclo de desenvolvimento seguro — versionamento, pipelines, repositórios, artefatos, dashboards, auditoria e análises SAST e DAST.

1.4.2.6.6 Segundo a pesquisa de mercado realizada, o GitHub é a solução que mais se aproxima do GitLab em termos de funcionalidades e suporte ao ciclo de desenvolvimento completo. No entanto, ainda requer integrações adicionais e não oferece o mesmo nível de unificação nativa, o que reforça que o GitLab permanece como a opção mais consolidada e completa para atendimento integral às necessidades do órgão.

1.4.2.6.7 Nesse contexto, a contratação da versão comercial do GitLab representa a alternativa tecnicamente mais sólida, economicamente sustentável no longo prazo e institucionalmente mais segura, equilibrando conformidade, continuidade, governança, redução de riscos e modernização da infraestrutura de desenvolvimento. Assim, conclui-se que a Solução 2 configura a opção mais adequada para atender de forma plena, eficiente e sustentável às necessidades operacionais e estratégicas da instituição.

1.4.3 CONTRATAÇÕES PÚBLICAS SIMILARES

1.4.3.1 Considerando a definição e a análise das alternativas disponíveis, a **licitação na modalidade pregão eletrônico** foi identificada como a solução adequada para atender ao objeto. Dessa forma, as referências apresentadas a seguir restringem-se exclusivamente a essa modalidade de contratação.

Rondônia (DPE-RO) - Doc. 1759395;

1.4.3.1.2 Pregão Eletrônico nº 5/2023 – Conselho da Justiça Federal (CJF) - Doc. 1757529;

1.4.3.1.3 Pregão Eletrônico nº 80/2023 – Superintendência Estadual de Compras e Licitações (SUPEL-RO) - Doc. 1759389;

1.4.3.1.4 Pregão Eletrônico nº 22/2024 – Ministério Público do Estado de Rondônia (MP-RO) - Doc. 1759391;

1.4.4 SOLUÇÕES SIMILARES EM OUTROS ÓRGÃOS

1.4.4.1 Nos termos do item 1.4.3.

1.4.5 MODELOS DE AQUISIÇÃO/PRESTAÇÃO DO SERVIÇO

1.4.5.1 Justificativa pela opção *on-premises*

1.4.5.1.1 Considerando que o GitLab já se encontra instalado e consolidado no ambiente *on-premises* do Tribunal desde 2018, em sua edição *Community Edition*, e que, ao longo desse período, foi incorporado progressivamente às rotinas institucionais de desenvolvimento, automação, homologação e controle de versões de software, conclui-se que a adoção do modelo de licenciamento *on-premises* representa a opção mais adequada e estratégica para o órgão.

1.4.5.1.2 A solução já está amplamente integrada ao fluxo de trabalho institucional, contando com significativos investimentos técnicos, capacitação de servidores e estruturação de pipelines, o que evidencia maturidade operacional no uso da ferramenta. A continuidade por meio da versão licenciada garante não apenas a preservação dos processos já consolidados, mas também maior controle sobre dados, integrações e políticas de segurança, sem provocar mudanças disruptivas na infraestrutura existente.

1.4.5.1.3 Dessa forma, a escolha pelo modelo *on-premises* revela-se tecnicamente viável, economicamente racional e institucionalmente vantajosa, assegurando a evolução natural da solução já adotada, em conformidade com as diretrizes de governança e segurança da informação do Tribunal.

1.4.5.2 Funcionalidades disponíveis nas versões comerciais do GitLab

1.4.5.2.1 O GitLab apresenta diferentes camadas de licenciamento, sendo as mais relevantes a versão **Premium** e a versão **Ultimate**. Abaixo, destacam-se as principais funcionalidades:

Funcionalidade	Disponível na Premium	Disponível na Ultimate
Controle de acesso granular com RBAC avançado	Sim	Sim
Autenticação via LDAP, SAML, OAuth com SSO	Sim	Sim
Painel de segurança com detecção de vulnerabilidades	Sim	Sim
Gerenciamento de Vulnerabilidade, Dashboards de Segurança, Políticas de Segurança, Análise de Composição de Software (SCA), Análise de IaC, Teste de fuzz e Testes Dinâmicos de Segurança	Não	Sim
SAST, DAST, Dependency Scanning, Container Scanning	Sim	Sim

Funcionalidade	Disponível na Premium	Disponível na Ultimate
Auditoria de ações de usuários (Audit logs)	Sim	Sim
Dashboard de compliance e licenças de pacotes	Sim	Sim
Value Stream Management (VSM) e epics multinível	Não	Sim
Criação e Acompanhamento de Casos de Teste	Não	Sim
Regras de push, permitindo forçar aderência a padrões estabelecidos	Sim	Sim
Guardrails para merge requests, permitindo definir revisores e criar fluxos de aprovação	Sim	Sim
Alta disponibilidade (HA) com suporte oficial	Sim	Sim
Suporte técnico especializado e atualizações de segurança	Sim	Sim

Tabela 3 – Funcionalidades disponíveis nas versões comerciais do GitLab

1.4.5.2.2 Justificativa pela versão Ultimate

1.4.5.2.2.1 A contratação da licença GitLab Ultimate configura-se como a alternativa mais adequada e estratégica para o Tribunal, tendo em vista a necessidade de evolução tecnológica da solução já consolidada em ambiente on-premises desde 2018. Embora a edição Premium contemple funcionalidades relevantes, a versão Ultimate disponibiliza um conjunto ampliado de recursos que atende, de forma mais abrangente, às demandas de segurança, conformidade e governança institucional.

1.4.5.2.2.2 Do ponto de vista técnico, a versão Ultimate viabiliza a plena adoção de práticas DevSecOps, com a incorporação de mecanismos avançados de automação de segurança, tais como SAST, DAST, *Dependency Scanning* e *Container Scanning*, além de recursos específicos de gerenciamento contínuo de vulnerabilidades, análise de composição de software (SCA), inspeção de código malicioso e detecção de segredos em repositórios. Esses elementos são fundamentais para a detecção precoce de riscos e a mitigação de falhas em todo o ciclo de desenvolvimento.

1.4.5.2.2.3 Sob a ótica de conformidade, a edição Ultimate alinha-se diretamente às boas práticas e normas internacionais, como os **CIS Controls v8** e a **ISO/IEC 27001**, garantindo aderência a requisitos de segurança da informação reconhecidos globalmente. Entre os controles mais relevantes contemplados estão a gestão contínua de vulnerabilidades, a implementação de mecanismos avançados de autenticação e autorização, e a rastreabilidade de incidentes por meio de auditoria detalhada das ações executadas na plataforma.

1.4.5.2.2.4 No aspecto de governança e gestão operacional, a versão Ultimate oferece funcionalidades que não estão presentes na edição Premium, como dashboards de conformidade, relatórios de licenciamento de pacotes, *Value Stream Management* e acompanhamento de casos de teste. Tais recursos ampliam a capacidade de monitoramento,

transparência e previsibilidade nos processos de desenvolvimento, resultando em maior eficiência e confiabilidade das entregas de software críticas ao Tribunal.

1.4.5.2.2.5 Assim, a opção pela versão Ultimate transcende a simples ampliação funcional da solução, representando medida estratégica para elevar o nível de maturidade em desenvolvimento seguro, fortalecer a resiliência cibernética institucional e assegurar a continuidade de serviços essenciais, de forma alinhada às diretrizes de segurança, eficiência e governança tecnológica da Administração Pública.

1.4.5.3 Outras providências relevantes

1.4.5.3.1 Contratação por meio de parceiro autorizado (revenda ou integrador)

1.4.5.3.1.1 A aquisição deverá ser realizada por intermédio de empresa parceira do fornecedor, habilitada como revenda ou integradora oficial.

1.4.6 CAPACIDADE E ALTERNATIVAS DO MERCADO DE TIC

1.4.6.1 O mercado de soluções DevOps apresenta fornecedores consolidados, porém limitado quanto à oferta de soluções capazes de atender a demandas complexas de ambientes on-premises integrados, como o do Tribunal Regional Eleitoral de Sergipe. Entre as alternativas disponíveis destacam-se o licenciamento em nuvem (SaaS) e o licenciamento on-premises.

1.4.6.2 Considerando que o GitLab se encontra em uso no ambiente on-premises do Tribunal desde 2018, com integração consolidada aos fluxos de trabalho, capacitação da equipe e investimentos prévios em infraestrutura e processos, a adoção da versão Ultimate em modelo on-premises configura a alternativa mais adequada e estratégica. Essa opção assegura continuidade operacional, aderência às normas e boas práticas de segurança da informação, governança tecnológica e eficiência nos processos de desenvolvimento, manutenção e controle de versões de software.

1.4.7 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

1.4.7.1 Não se aplica.

1.5 ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA

1.5.1 Com base nas consultas de preços realizadas no mercado, a partir do Termo de Referência elaborado para esta contratação, estima-se que o custo total da demanda compreenderá a **aquisição de licenças de uso do software GitLab Ultimate Edition**, para **40 (quarenta) usuários nomeados ativos**, com período de vigência de **12 (doze) meses**.

Id	Fornecedor	Período	Valor unitário (R\$)	Documento
1	BK Tecnologia da Informação	12 meses	R\$ 8.850,00	PE 90019/2024 (1763117)
2	DELFINA S/A	12 meses	R\$ 8.630,00	PE 80/2023 1763124
3	BK Tecnologia da Informação	12 meses	R\$ 15.450,00	Proposta (1764032)

Tabela 4 - Pesquisa de mercado

1.6 ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

1.6.1 DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

1.6.1.1 A solução escolhida, GitLab Ultimate em modelo on-premises, foi definida considerando a consolidação da plataforma no ambiente do Tribunal desde 2018, a maturidade operacional da equipe e a integração aos fluxos institucionais de desenvolvimento, automação e controle de versões.

1.6.1.2 A versão Ultimate oferece recursos avançados de segurança, conformidade e governança, incluindo automação de testes, gerenciamento de vulnerabilidades, rastreabilidade de incidentes e dashboards de compliance, alinhados a normas como ISO/IEC 27001 e CIS Controls v8.

1.6.1.3 Além disso, a solução on-premises aproveita a infraestrutura existente, garantindo controle sobre dados, integrações e políticas de segurança, assegurando continuidade operacional, eficiência e confiabilidade nos serviços essenciais do Tribunal.

1.6.2 BENEFÍCIOS ESPERADOS

1.6.2.1 Continuidade operacional com aproveitamento da infraestrutura e equipe já capacitada.

1.6.2.2 Fortalecimento da segurança, conformidade e práticas DevSecOps.

1.6.2.3 Transparência e governança nos processos de desenvolvimento.

1.6.2.4 Maior eficiência, produtividade e colaboração entre equipes.

1.6.2.5 Resiliência cibernética e mitigação de riscos.

1.6.2.6 Autonomia para personalização e integração institucional.

1.6.3 RESULTADOS ESPERADOS

1.6.3.1 Manutenção estável da solução já implantada desde 2018.

1.6.3.2 Automação de testes de segurança, rastreabilidade e conformidade com normas internacionais.

1.6.3.3 Dashboards de compliance, gestão de vulnerabilidades e controle de acessos.

1.6.3.4 Pipelines otimizados, integração contínua e entregas confiáveis.

1.6.3.5 Detecção antecipada de falhas e resposta rápida a incidentes.

1.6.3.6 Integração plena com sistemas internos e proteção de dados sensíveis.

1.6.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS E/OU SERVIÇOS CONTRATADOS

1.6.4.1 A demanda prevista tem respaldo na quantidade de usuários aptos a utilizar a ferramenta:

Unidade	Qtd usuários
STI	1
ASPLAN-STI	1
ASSEC	3

NAC	1
SEAPU	6
SESOP	6
NAI	5
SEAUE	2
COINF	1
COSIS	1
SEADA	4
SEJUD	2
SESEL	4
NAS	1
ASCID	2
TOTAL	40

Tabela 5 - Demanda prevista

1.6.4.2 Ressalta-se que o contrato poderá ser objeto de aditivos na hipótese de ampliação do quadro de pessoal, seja pela posse de novos servidores, seja pela contratação de colaboradores.

1.7 DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

1.7.1 O presente ESTUDO TÉCNICO PRELIMINAR foi elaborado pela(o)s integrantes TÉCNICA(O) e DEMANDANTE, em harmonia com a Resolução CNJ Nº 468 de 15/07/2022.

1.7.2 Considerando a análise das alternativas de atendimento das necessidades elencadas pela área demandante e os demais aspectos normativos, conclui-se pela VIABILIDADE DA CONTRATAÇÃO da versão Ultimate do GitLab em modelo on-premises, que se mostra estratégica por aproveitar a infraestrutura existente e os investimentos já realizados desde 2018, garantindo continuidade operacional, segurança e conformidade com normas internacionais. Ademais, a medida fortalece a governança tecnológica, a eficiência no desenvolvimento de sistemas e a resiliência cibernética do Tribunal, assegurando benefícios em termos de eficácia, eficiência, efetividade e economicidade, dos quais citam-se nominalmente:

- a) Garantir a continuidade adequada dos serviços do TRE-SE, em atendimento às necessidades do órgão e do público;
- b) Manter a disponibilidade das exigências de qualidade dos serviços, possibilitando o melhoramento do atendimento das demandas de acordo com sua criticidade.

1.7.3 Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que SE RECOMENDA o prosseguimento da pretensão contratual.

2. CAPÍTULO 2: SUSTENTAÇÃO DO CONTRATO

2.1 ADEQUAÇÃO DO AMBIENTE

2.1.1 Não se aplica.

2.2 RECURSOS MATERIAIS E HUMANOS

2.2.1 Recursos Materiais

2.2.1.1 Não se aplica.

2.2.2 Recursos Humanos

2.2.2.1 Os recursos humanos serão compostos exclusivamente pelas(os) servidoras(es) da seção, bem como por terceirizadas(os) e estagiárias(os) disponíveis para a seção.

2.3 CONTINUIDADE DO FORNECIMENTO

2.3.1 Manutenção da Instância Atual (Free) como Base de Transição:

a) Garantir que a instância GitLab Free existente seja preservada até a conclusão da implantação da versão Ultimate.

b) Realizar backup completo dos repositórios, pipelines e configurações.

c) Definir cronograma de migração para evitar interrupção dos serviços.

2.3.2 Licenciamento e Renovação Contínua:

a) Estabelecer contrato com vigência plurianual ou com cláusulas de renovação, mitigando riscos de descontinuidade no fornecimento das licenças Ultimate.

b) Prever, no contrato, prazos adequados para renovação antes do vencimento da licença.

2.3.3 Suporte Técnico e Atualizações:

a) Garantir suporte oficial do fornecedor durante todo o período contratual (atualizações de segurança, correções de bugs, novas funcionalidades).

b) Adoção de boas práticas de gestão de versão e atualização programada do software, evitando vulnerabilidades e obsolescência.

2.3.4 Plano de Contingência:

a) Caso a edição *Ultimate* venha a ser descontinuada pelo fabricante ou se torne economicamente inviável sua manutenção na infraestrutura atual, a equipe técnica deverá avaliar e conduzir a migração para solução alternativa que assegure a continuidade dos serviços, observando requisitos de interoperabilidade, segurança e integridade dos repositórios.

b) Definir estratégias de redundância (backups regulares e ambientes de teste).

2.4 TRANSIÇÃO CONTRATUAL E ENCERRAMENTO DO CONTRATO

2.4.1 A transição contratual deverá ser planejada de forma a assegurar que, ao término da vigência do contrato, não haja interrupção dos serviços essenciais providos pela solução GitLab Ultimate. Para tanto, serão observados os seguintes aspectos:

2.4.1.1 Planejamento Antecipado

a) Iniciar, com antecedência mínima de 150 dias, o processo de renovação contratual ou de nova contratação, de forma a evitar descontinuidade de licenciamento, suporte e atualizações.

b) Estabelecer prazo de, no máximo, 120 dias antes do término da vigência contratual para a formalização da decisão sobre renovação, substituição ou encerramento definitivo.

2.4.1.2 Reversibilidade e Continuidade dos Serviços

- a) Garantir que todos os repositórios, pipelines, configurações e históricos armazenados no GitLab Ultimate possam ser exportados e preservados em caso de migração ou retorno à versão Free.
- b) Documentar procedimentos para transição técnica, assegurando que os serviços do TRE-SE continuem disponíveis sem impactos significativos.

2.4.1.3 Encerramento Organizado

- a) No caso de não renovação, assegurar que os dados sejam entregues de forma íntegra e em formatos abertos ou compatíveis, preservando a integridade do histórico e da rastreabilidade dos projetos.
- b) Estabelecer mecanismos de verificação de conformidade no encerramento, garantindo que não haja perda de ativos digitais ou risco à segurança da informação.

2.5 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA

2.5.1 A contratação da versão Ultimate do GitLab, em modelo on-premises, será conduzida de forma a mitigar riscos de dependência tecnológica excessiva do fornecedor, observando-se os seguintes aspectos:

2.5.1.1 Adoção de Padrões Abertos e Interoperabilidade

- a) O GitLab utiliza protocolos e formatos amplamente reconhecidos (como Git e APIs REST/GraphQL), garantindo a possibilidade de integração com outras ferramentas e a migração de dados sem perda de integridade.

2.5.1.2 Reversibilidade e Portabilidade

- a) Os repositórios de código, pipelines e configurações podem ser exportados para outros sistemas compatíveis com Git, assegurando a possibilidade de migração futura para soluções alternativas, sejam comerciais ou de código aberto.

2.5.1.3 Redução de Dependência Exclusiva

- a) O uso do GitLab Ultimate on-premises preserva o controle da infraestrutura no âmbito do TRE-SE, eliminando a dependência de serviços totalmente externos (cloud-only).
- b) A equipe técnica terá autonomia para administrar a solução, sem restrições impeditivas de uso, customização ou migração.

2.5.1.4 Capacitação Interna

- a) Haverá treinamento contínuo das equipes de TI para operação, administração e manutenção da solução, garantindo que o conhecimento não fique concentrado apenas no fornecedor.

2.5.1.5 Planejamento de Alternativas Futuras

- a) O TRE-SE manterá monitoramento das condições de mercado e das soluções concorrentes, possibilitando a avaliação periódica de alternativas tecnológicas e garantindo maior poder de negociação em futuras contratações.

3. CAPÍTULO 3: ESTRATÉGIA PARA A CONTRATAÇÃO

REQUISITOS	AVALIAÇÃO
------------	-----------

REQUISITOS	AVALIAÇÃO
3.1 Natureza do objeto	<input type="checkbox"/> compra <input checked="" type="checkbox"/> fornecimento contínuo <input type="checkbox"/> serviços contínuos sem regime de dedicação exclusiva de mão de obra <input type="checkbox"/> serviços contínuos com regime de dedicação exclusiva de mão de obra <input type="checkbox"/> serviços não contínuos ou contratados por escopo <input type="checkbox"/> Outros: _____
3.2 Enquadramento como bem/ serviço comum ou especial	<input checked="" type="checkbox"/> bens/serviços comuns <input type="checkbox"/> bens/serviços especiais <input type="checkbox"/> serviços técnicos especializados de natureza predominantemente intelectual <input type="checkbox"/> Outros: _____
3.3 Regime de contratação recomendado	<input type="checkbox"/> empreitada por preço unitário <input checked="" type="checkbox"/> empreitada por preço global <input type="checkbox"/> Outros: _____
3.4 Vigência da contratação	Vigência de 12 (doze) meses , compatível com a necessidade imediata da STI e com os prazos previstos no planejamento orçamentário.
3 . 5 Forma/meio de contratação recomendada	<input checked="" type="checkbox"/> Licitação <input type="checkbox"/> Dispensa de licitação <input type="checkbox"/> Inexigibilidade de licitação <input type="checkbox"/> Adesão a ata de registro de preços <input type="checkbox"/> Participação em compra compartilhada <input type="checkbox"/> Outros: _____
3 . 6 Modalidade de licitação (art. 28, inciso I, c/c art. 29, da Lei 14.133/2021)	<input checked="" type="checkbox"/> Pregão <input type="checkbox"/> Concorrência <input type="checkbox"/> Concurso <input type="checkbox"/> Leilão <input type="checkbox"/> Diálogo competitivo

REQUISITOS	AVALIAÇÃO
3.7 Adoção de Sistema de Registro de Preços (SRP)	<input type="checkbox"/> Sim <input checked="" type="checkbox"/> Não
3.7.1 Utilização da Intenção de Registro de Preços (IRP)	Não se aplica
3.7.2 Permissão à Adesão à Ata de Registro de Preços	Não se aplica
3.8 Parcelamento do objeto	<input type="checkbox"/> Parcelado. <input checked="" type="checkbox"/> Não parcelado. <i>Justificativa:</i> Nos termos do art. 40, §§ 2º e 3º, e art. 47, § 1º, da Lei nº 14.133/2021, o parcelamento da contratação deve ser avaliado quanto à viabilidade técnica e à vantajosidade econômica para a Administração. Após análise das características da solução a ser contratada, justifica-se a inviabilidade do parcelamento do objeto , uma vez que o software (GitLab Ultimate Edition) deve ser contratado em licenciamento integral, para garantir cobertura de suporte, padronização tecnológica e compatibilidade com os ambientes do TRE-SE.
3.9 Adjudicação do objeto	<input type="checkbox"/> menor preço por grupo de itens (lote) <input checked="" type="checkbox"/> menor preço por item <input type="checkbox"/> maior desconto
3.10 Tratamento diferenciado para ME/EPP	<input checked="" type="checkbox"/> Sim <input type="checkbox"/> Não <i>Justificativa:</i>
3.11 Caráter sigiloso do orçamento estimado	<input type="checkbox"/> Sim <input checked="" type="checkbox"/> Não <i>Justificativa:</i> Para preservar a competitividade, conforme art. 24, §1º da Lei 14.133/2021.

REQUISITOS	AVALIAÇÃO
3.12 Participação de consórcios	<input type="checkbox"/> Permitida <input checked="" type="checkbox"/> Vedada <i>Justificativa:</i> A participação em consórcios não é adequada, considerando que o objeto envolve licenciamento de software de fornecedores oficiais, cuja comercialização já ocorre por meio de canais autorizados. A formação de consórcios não agregaria competitividade e poderia aumentar riscos de gestão contratual.
3.13 Participação de sociedades cooperativas	<input checked="" type="checkbox"/> Permitida <input type="checkbox"/> Vedada <i>Justificativa:</i> Desde que devidamente credenciadas como representantes autorizadas ou revendedoras oficiais dos fabricantes, sociedades cooperativas poderão participar, atendendo integralmente aos requisitos contratuais.
3.14 Subcontratação	<input type="checkbox"/> Permitida <input checked="" type="checkbox"/> Vedada <i>Justificativa:</i> A subcontratação está vedada, pois o contrato deve assegurar a prestação dos serviços diretamente pela empresa contratada, que deverá ser representante ou revendedora oficial do fabricante, garantindo autenticidade e validade das licenças, bem como suporte técnico adequado.
3.15 Vistoria prévia	<input type="checkbox"/> Necessária <input checked="" type="checkbox"/> Dispensada <i>Justificativa:</i> A execução do contrato refere-se a licenciamento de software com suporte remoto, não sendo necessária vistoria técnica prévia.
3.16 Apresentação de amostras, exames de conformidade ou provas de conceito	<input type="checkbox"/> Sim. <i>Critérios:</i> <input checked="" type="checkbox"/> Não
3.17 Critérios de qualificação fornecedor - HABILITAÇÃO JURÍDICA	<input checked="" type="checkbox"/> É obrigatória a autorização para o exercício da atividade a ser contratada. <input type="checkbox"/> NÃO É obrigatória a autorização para o exercício da atividade a ser contratada.
3.18 Critérios de qualificação fornecedor - TÉCNICA-OPERACIONAL E TÉCNICA-PROFISSIONAL	<input type="checkbox"/> SIM. <i>Detalhes:</i> <input checked="" type="checkbox"/> NÃO <i>Justificativa:</i> Considerando que o objeto é licenciamento de software de prateleira, com suporte prestado diretamente pelo fabricante ou representante autorizado, não se faz necessária a exigência de atestados técnicos adicionais, sendo suficiente a comprovação de representação oficial.

REQUISITOS	AVALIAÇÃO
3.19 Critérios de qualificação do fornecedor ECONÔMICO-FINANCEIRA	X SIM. <i>Detalhes:</i> O(A) licitante deverá apresentar certidão negativa de feitos sobre falência expedida pelo distribuidor da sede da(o) licitante, conforme art. 69, inciso II, da Lei 14.133/2021. <input type="checkbox"/> Não
3.20 Garantia de proposta	<input type="checkbox"/> Sim. <i>Detalhes:</i> X Não
3.21 Garantia de execução contratual	<input type="checkbox"/> Sim. <i>Detalhes:</i> X Não <i>Justificativa:</i> Considerando que se trata de contratação de licenciamento de software com serviços acessórios, cujo pagamento será efetuado após a disponibilização das licenças e a validação da prestação de suporte , não se faz necessária a exigência de garantia de execução contratual.
3.22 Classificação do conteúdo do estudo técnico	<input type="checkbox"/> Restrito <input type="checkbox"/> Sigiloso <input type="checkbox"/> Confidencial <input type="checkbox"/> Secreto X Público
3.23 Margem de preferência	<input type="checkbox"/> Sim. <i>Detalhes:</i> X Não <i>Justificativa:</i> A solução contratada é software proprietário internacional (GitLab), não havendo margem de preferência aplicável no mercado nacional.
3.24 Equipe de apoio à contratação	Integrantes Demandantes <ul style="list-style-type: none"> • Titular: Fernando de Souza Lima (NAC/STI) • Substituto(a): Martha Coutinho de Faria Alves (NAI/STI) Integrantes Técnicos <ul style="list-style-type: none"> • Titular: Diego Medeiros Vilar Oliveira (SESEL/STI) • Substituto(a): Jeirlan Correia Palmeira (COSIS/STI) Integrantes Administrativos <ul style="list-style-type: none"> • Titular: Ricardo Loeser de Carvalho Filho (ASPLAN-SAO) • Substituto(a): Valéria Maria dos Santos (ASPLAN-SAO)

REQUISITOS	AVALIAÇÃO
3.25 Equipe de gestão do contrato	<p>Gestor(a)</p> <ul style="list-style-type: none"> • Titular: Fernando de Souza Lima (NAC/STI) • Substituto(a): Martha Coutinho de Faria Alves (NAI/STI) <p>Fiscais Técnicos</p> <ul style="list-style-type: none"> • Titular: Diego Medeiros Vilar Oliveira (SESEL/STI) • Substituto(a): Jeirlan Correia Palmeira (COSIS/STI) <p>Fiscais Administrativos</p> <ul style="list-style-type: none"> • Titular: Ricardo Loeser de Carvalho Filho (ASPLAN-SAO) • Substituto(a): Valéria Maria dos Santos (ASPLAN-SAO)
3.26 Capacitação da Equipe de gestão do contrato	<p><input type="checkbox"/> Há necessidade de capacitação.</p> <p><input checked="" type="checkbox"/> Não há necessidade de capacitação.</p>
3.27 Outras informações relevantes (exemplo: Política de Segurança da Informação e Privacidade; Critérios de sustentabilidade exigidos; etc)	<p>A contratação observará a Política de Segurança da Informação e Privacidade da Justiça Eleitoral e as boas práticas de sustentabilidade definidas nas normas do TCU e no Plano de Logística Sustentável (PLS) do TRE-SE.</p>

4. CAPÍTULO 4: ANÁLISE DE RISCOS

4.1 RISCOS MAPEADOS

	Risco:	Impossibilidade manter a solução por um longo periodo
	Probabilidade:	Média
	Impacto:	Muito alto
	Dano 1:	Reversão para a versão <i>free</i> , resultando na perda de funcionalidades avançadas de segurança e outras
	Dano 2:	Indisponibilidade parcial dos sistemas atualmente suportados pela solução, caso seja necessária a adoção de uma nova plataforma sem plena equivalência funcional.
	Tratamento:	Mitigar

Risco 01	Id	Ação Preventiva	Responsável
	1	Planejamento orçamentário plurianual dedicado à manutenção da solução , garantindo previsibilidade de recursos para renovações.	EGC
	2	Monitoramento contínuo de prazos contratuais e de vigência da assinatura , com alertas automáticos para renovação com antecedência mínima.	EGC
	3	Negociação de contratos com cláusulas de renovação e reajustes previsíveis , reduzindo incertezas e riscos de interrupção financeira.	EGC
	4	Criar rotinas de backup e versionamento abrangentes , incluindo dados, repositórios, pipelines e configurações.	Equipe Técnica
	Id	Ação de Contingência	Responsável
	1	Manter a versão free	Equipe Técnica
	2	Planejamento da migração	Equipe Técnica

5. APROVAÇÃO E ASSINATURA

INTEGRANTES TÉCNICOS

JEIRLAN CORREIA PALMEIRA

Matrícula: 30923144
Aracaju, datado e assinado eletronicamente

INTEGRANTE DEMANDANTE

FERNANDO DE SOUZA LIMA

Matrícula: 30923292
Aracaju, datado e assinado eletronicamente

6. CIÊNCIA DA INSTÂNCIA DELIBERATIVA DE TIC

AUTORIDADE MÁXIMA DA ÁREA DE TIC

JOSÉ CARVALHO PEIXOTO

Secretário de TIC
Matrícula: 309R639

Anexo A – Lista de Potenciais Fornecedores

	FORNECEDOR
1	Razão social do fornecedor 1 - BK TECNOLOGIA DA INFORMAÇÃO LTDA Site: E-mail: edison@bktech.com.br Telefone: (61) 98136-7690
2	Razão social do fornecedor 2 - DELFIA S/A Site: E-mail: licitacao@delfia.tech Telefone: (61) 98160-5194
3	Razão social do fornecedor N Site: E-mail: Telefone: (DDD) xxxx-xxxx

Anexo B – Propostas Comerciais

a) Doc. 1764032.

Anexo C – Contratações Públicas Similares

a) Conforme item 1.4.3.



Documento assinado eletronicamente por **JEIRLAN CORREIA PALMEIRA**, Integrante da EPC Titular, em 09/12/2025, às 08:31, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **FERNANDO DE SOUZA LIMA, Integrante da EPC Titular**, em 09/12/2025, às 08:38, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **JOSÉ CARVALHO PEIXOTO, Secretária(o)**, em 09/12/2025, às 10:46, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **VALÉRIA MARIA DOS SANTOS, Assessor(a)**, em 09/12/2025, às 10:49, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ANA MARIA RABELO DE CARVALHO DANTAS, Diretor(a)-Geral em Substituição**, em 09/12/2025, às 11:24, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-se.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1788340** e o código CRC **4724979B**.