

TERMO DE REFERÊNCIA

Processo Digital no. 412/2025

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Objeto

- 1.2. Contratação da subscrição de licenças da ferramenta GitLab Ultimate, totalizando 100 licenças pelo período de 24 meses, juntamente com serviços técnicos correlatos de implantação, migração, consultoria técnica, treinamento e operação assistida, para atender às necessidades específicas da Assembleia Legislativa do Estado de São Paulo (ALESP).
- 1.3. O prazo de vigência do contrato será de 24 (vinte e quatro) meses, contados a partir da assinatura do contrato, podendo ser prorrogado por iguais e sucessivos períodos, conforme o disposto no inciso II do art. 107 da Lei nº 14.133/2021, desde que mantidas as condições vantajosas para a Administração
- 1.4. Todo o escopo do objeto, envolvendo os diversos ambientes contemplados, deverá ser fornecido por uma só empresa (lote único) por questões técnicas e econômicas estratégicas. O agrupamento dos itens em lote único considera questões técnicas e estratégicas, tais como: premissa de operação integrada e sincronizada de todos os serviços visando garantir de forma efetiva os objetivos de performance, implementação, migração, otimização operacional, estabilidade e garantia manutenção preventiva, corretiva e evolutiva para todo conjunto, ganho de economia em escala, conforme análise detalhada realizada no Estudo Técnico Preliminar.
- 1.5. O regime de execução do contrato será de EMPREITADA POR PREÇO GLOBAL para os itens 1, 2, 3, 5 e 6. Para o item 4, o regime de execução será de EMPREITADA POR PREÇO UNITÁRIO. Também, é considerado serviço associado, de natureza CONTINUADA, classificado como COMUM, o item 6.
- 1.6. É vedada a subcontratação dos serviços objeto desta contratação.
- 1.7. Todos os custos necessários para a completa realização dos serviços (fornecimento) especificados neste Termo de Referência deverão ser contemplados na Proposta Comercial da licitante, de tal modo que, sendo CONTRATADA, tenha condições de realizar a totalidade das atividades previstas em contrato, sem ônus adicionais para a ALESP.
- 1.8. O presente descritivo contempla especificações técnicas e funcionais precisas, suficientes e claras para atender na íntegra as demandas

desta Casa, não contendo qualquer excesso que frustre a competitividade, ou ainda, inviabilize a participação dos interessados.

- 1.9. A análise dos riscos que possam comprometer o sucesso da licitação e a boa execução contratual encontra-se em documento apartado e apenso ao processo.
- 1.10. No que tange a utilização do Catálogo Eletrônico de Padronização, previsto no inciso II do Artigo 19 da Lei Federal n.º 14.133/2021 e no Artigo 10 do Decreto Estadual n.º 68.021/2023, catálogo esse que se encontra no portal eletrônico “compras.gov”, fica declarado que não existe a possibilidade de utilizá-lo, pois o objeto desta contratação não está presente no referido Catálogo.
- 1.11. Caso haja dúvidas sobre as informações aqui contidas, as empresas participantes deverão dirigir-se ao Departamento de Tecnologia da Informação, por meio do telefone (11) 3886-6448, para que as dúvidas sejam esclarecidas.

1.12. Quadro com os serviços e volumes que compõem o objeto

Item	Descrição	Quantidade	Unidade
1	Licenças GitLab Ultimate	100 (por 24 meses)	Licenças
2	Implantação da Plataforma GitLab Ultimate	1	Serviço
3	Migração	1	Serviço
4	Consultoria (DevSecOps, Processos, Gestão)	300	Horas Técnicas
5	Treinamento	50	Usuário Treinado
6	Operação assistida	24	Meses

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

- 2.1. A Assembleia Legislativa do Estado de São Paulo (ALESP), por meio da Divisão de Sistemas e Soluções, executa diversas atividades relacionadas ao desenvolvimento, manutenção e operação de sistemas institucionais críticos, responsáveis pelo suporte às atividades legislativas e administrativas. A eficiência, segurança e agilidade dessas atividades impactam diretamente na capacidade operacional e na prestação de serviços da ALESP.
- 2.2. Atualmente, as equipes técnicas utilizam a versão gratuita do GitLab, plataforma já consagrada para a gestão do ciclo de vida do desenvolvimento de software, abrangendo o controle de versões, documentação técnica, gerenciamento de projetos e automações básicas de integração e entrega contínuas (CI/CD). Contudo, essa versão não contempla funcionalidades essenciais para atender plenamente às demandas crescentes da ALESP, sobretudo no tocante à segurança cibernética avançada, compliance com normas e regulamentos técnicos, gestão aprimorada de projetos e gerenciamento de vulnerabilidades.
- 2.3. A Divisão de Sistemas e Soluções da ALESP participou de um assessment técnico conduzido em parceria com especialistas em GitLab, cujo objetivo foi avaliar o grau de maturidade das práticas DevOps na instituição, identificar gargalos operacionais e estabelecer recomendações para evolução da plataforma GitLab.
- 2.4. O diagnóstico evidenciou que, embora o GitLab seja utilizado internamente desde 2016, sua aplicação ainda é restrita à gestão de código fonte (SCM) e utilização básica de CI/CD, sem integração com segurança, infraestrutura ou gestão ágil de projetos. A esteira atual apresenta gargalos, ausência de boas práticas de desenvolvimento, baixa cobertura de testes automatizados e inexistência de processos de validação em segurança.
- 2.5. A cadeia de ferramentas utilizada está fragmentada, com uso de Nexus, Docker Swarm e Trello em paralelo e sem integração com o GitLab, o que gera retrabalho, perda de rastreabilidade e baixa governança dos projetos. Adicionalmente, não há processos definidos para gestão de vulnerabilidades, conformidade de licenças, auditoria de código ou proteção da cadeia de suprimentos.
- 2.6. Entre os principais riscos diagnosticados, destacam-se: retrabalho recorrente, risco de não conformidade regulatória, exposição de propriedade intelectual e aumento de custos operacionais.
- 2.7. Como resultado do assessment, foram propostas diretrizes e recomendações estratégicas, tais como:
 - 2.7.1. Consolidação da cadeia de ferramentas no GitLab, substituindo ou integrando sistemas legados;

- 2.7.2. Implantação de práticas de DevSecOps com validação de segurança automatizada (SAST, DAST, SCA, Secret Detection, Container Scanning);
- 2.7.3. Ampliação do uso do GitLab para gestão de projetos, planejamento ágil e indicadores (DORA metrics, Value Stream);
- 2.7.4. Estabelecimento de fluxos de aprovação e políticas automatizadas para falhas críticas;
- 2.7.5. Expansão da plataforma para contemplar equipes de segurança, infraestrutura e operações;
- 2.7.6. Criação de processos formais de governança, auditoria e conformidade no ciclo de vida das aplicações;
- 2.7.7. Suporte à migração de infraestrutura (ex: Nexus para GitLab Registry, Docker Swarm para Kubernetes);
- 2.7.8. Capacitação técnica de administradores e usuários e definição de um modelo de administração contínua da solução.
- 2.8. A necessidade de contratação da versão GitLab Ultimate decorre, portanto, da crescente complexidade tecnológica e dos desafios regulatórios enfrentados pela ALESP, sobretudo com a intensificação do uso de aplicações digitais no ambiente legislativo. A versão Ultimate inclui funcionalidades exclusivas que aprimoram significativamente o controle, a segurança e a gestão do desenvolvimento de software, tais como ferramentas avançadas de auditoria e compliance, gestão automatizada e eficiente de vulnerabilidades e relatórios detalhados de segurança. Estas funcionalidades são essenciais para garantir a conformidade das aplicações institucionais com as exigências legais, técnicas e de segurança vigentes.
- 2.9. Além disso, a solução GitLab Ultimate disponibiliza recursos robustos para aumentar a produtividade das equipes de desenvolvimento, através de automações avançadas de processos, análise detalhada de desempenho, gestão de recursos e melhores práticas de governança de tecnologia da informação.
- 2.10. Portanto, a contratação das licenças GitLab Ultimate é necessária para mitigar riscos técnicos e operacionais, assegurar a qualidade, segurança e eficiência no desenvolvimento de soluções digitais e cumprir as exigências regulatórias e de compliance impostas pela legislação vigente, garantindo, assim, a continuidade e melhoria dos serviços oferecidos pela ALESP à sociedade.

3. DESCRIÇÃO DO SISTEMA COMO UM TODO

- 3.1. Trata-se de contratação de empresa especializada para fornecimento, de licenças (modelo de subscrição) da ferramenta GitLab Ultimate, incluindo os serviços de implantação, configuração e suporte técnico com direito à atualização de versão.

- 3.2. A contratação da solução GitLab Ultimate deverá abranger, além do fornecimento das licenças, um conjunto estruturado de serviços especializados que garantam a sua efetiva implementação, adoção, utilização estratégica e sustentação contínua. A seguir, detalham-se os macro itens que compõem esse escopo, com a descrição de suas respectivas atividades.

3.3. Licenças GitLab Ultimate

- 3.3.1. Fornecimento, pelo período de 24 (vinte e quatro) meses, de 100 (cem) licenças (modelo de subscrição) da ferramenta GitLab Ultimate, incluindo suporte e garantia, conforme descrito.
- 3.3.2. Os serviços de suporte na modalidade Priority Support detalhados em <https://about.gitlab.com/support/#priority-support> a serem contratados com fundamento neste Termo de Referência, deverão observar os seguintes requisitos mínimos obrigatórios:
- 3.3.2.1. Direito de atualização de versão pelo site do fabricante, caso uma nova versão do software venha a ser lançada, durante a vigência do contrato, sem ônus adicional para a CONTRATANTE.
- 3.3.2.1.1. Define-se atualização de versão como direito para atualização dos softwares, incluindo versões maiores (major releases), versões menores (minor releases), versões de manutenção (maintenance releases) e atualizações (updates) que forem disponibilizadas para os softwares contratados.
- 3.3.2.1.2. As novas versões da solução fornecida, bem como quaisquer outros componentes necessários ao adequado funcionamento, deverão ser disponibilizadas via internet, no prazo de até 2 (dois) dias consecutivos, contados da data do lançamento.
- 3.3.2.2. Direito ao serviço de suporte técnico para um número ilimitado de chamados durante a vigência do contrato, sem ônus adicional para a CONTRATADA.
- 3.3.2.2.1. Define-se serviço de suporte técnico como sendo aquele efetuado mediante atendimento telefônico e correio eletrônico, com objetivo de solucionar problemas de funcionamento e disponibilidade da solução e de esclarecer dúvidas relacionadas a instalação, configuração, uso e atualização dos produtos.
- 3.3.2.2.2. A CONTRATADA deverá disponibilizar canal de atendimento para abertura de chamados técnicos, mediante sistema Web ou de um telefone 0800.

- 3.3.2.2.3. Para cada chamado técnico, deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.
- 3.3.2.2.4. Os chamados técnicos serão categorizados em níveis de severidade conforme Priority Support detalhados em <https://about.gitlab.com/support/#priority-support>.
- 3.3.2.2.5. O nível de severidade dos chamados deverá ser comunicado à CONTRATADA no momento de sua abertura.
- 3.3.2.2.6. O chamado técnico só será considerado concluído após confirmação da CONTRATANTE.
- 3.3.2.2.7. O nível de severidade de um chamado poderá ser reclassificado e, nesse caso, haverá nova contagem de prazo, conforme o novo nível de severidade.
- 3.3.3. A CONTRATADA deverá apresentar, mensalmente, ou através de sistema WEB, relatório contendo as informações de data e hora de abertura e fechamento do chamado, nome do responsável pela abertura, nome do responsável pelo atendimento, número de controle (protocolo), nível de severidade e descrição sucinta do chamado.

3.4. Implantação da Plataforma GitLab Ultimate

- 3.4.1. Para que a CONTRATANTE possa aproveitar plenamente os recursos oferecidos pelo GitLab, é necessário realizar a instalação GitLab Ultimate na infraestrutura da Assembleia Legislativa do Estado de São Paulo e uma configuração inicial do ambiente, garantindo a disponibilidade e a integração adequada das ferramentas necessárias para o gerenciamento de projetos, integração contínua (CI) e entrega contínua (CD). Além de treinamento para que se possa aproveitar ao máximo os recursos oferecidos pela ferramenta. A seguir, são apresentadas as etapas e as ferramentas envolvidas nesse processo:
 - 3.4.1.1. A instalação deverá ser realizada no datacenter da CONTRATANTE (On-premise), no ambiente de produção.
 - 3.4.1.2. O ambiente de produção deverá contar com Estratégia de Recuperação Gradual (Cold Stand-by), para lidar com falhas ou interrupção dos serviços.
 - 3.4.1.3. Configurar o GitLab para alta disponibilidade possibilitando a atualização de versões sem tempo paralisado.
 - 3.4.1.4. Configurar e integrar executores de CI (por exemplo, GitLab CI/CD Runner) para processar os pipelines de integração contínua dimensionados para a demanda de uso avaliada pela CONTRATADA.

- 3.4.1.5. Habilitar o Security Dashboard no GitLab para monitorar e analisar a postura de segurança dos projetos em andamento.
- 3.4.1.6. Habilitar o Vulnerability Management para identificar e gerenciar vulnerabilidades de segurança em dependências de software utilizadas nos projetos.
- 3.4.1.7. Habilitar o Dependency Scanning para analisar as dependências de software e identificar possíveis problemas de segurança ou vulnerabilidades.
- 3.4.1.8. Habilitar o Container Scanning para verificar a segurança dos containers utilizados no processo de implantação.
- 3.4.1.9. Habilitar o Static Application Security Testing para analisar o código-fonte em busca de possíveis vulnerabilidades de segurança.
- 3.4.1.10. Habilitar o Dynamic Application Security Testing para identificar possíveis vetores de ataque nas aplicações.
- 3.4.1.11. Habilitar o Incident Management para rastrear e resolver incidentes relacionados à segurança e aos problemas do projeto.
- 3.4.1.12. Habilitar o Secret detection para identificar tokens e chaves de acesso de api expostas em código.
- 3.4.1.13. Configurar e habilitar o uso de páginas de projetos e grupos (GitLab Pages) possibilitando a documentação do projeto e/ou outras necessidades dentro da própria ferramenta.
- 3.4.1.14. Habilitar os demais recursos e ferramentas do plano Ultimate do GitLab para o gerenciamento de projeto e CI/CD, garantindo uma experiência completa e a maximização dos benefícios oferecidos pela plataforma.
- 3.4.1.15. Habilitar a busca global de código através da solução disponibilizada pelo GitLab Ultimate em ambiente self-managed também instalado e disponibilizado pela CONTRATADA.
- 3.4.1.16. O software deverá permitir a visualização prévia dos aplicativos (versões de patch, homologação e branches) pelas áreas de negócio durante o desenvolvimento.
- 3.4.1.17. Ao término da fase de implantação e configuração do GitLab Self-Managed no ambiente local da empresa, a CONTRATADA será responsável por realizar uma transferência de conhecimento abrangente à equipe de Tecnologia da Informação (TI) da CONTRATANTE. Esta etapa visa assegurar que a equipe interna esteja adequadamente capacitada para administrar, manter e otimizar a solução implementada.

3.5. Assistência à Migração

- 3.5.1. A assistência à migração consiste em um conjunto estruturado de atividades que visam garantir a transição segura, eficiente e ininterrupta do ambiente atual da ALESP para a nova instância do GitLab Ultimate em modelo on-premise, contemplando os aspectos técnicos, operacionais e de integração com o ecossistema já existente. Esta etapa é crítica para assegurar a continuidade das operações, a integridade dos dados e o aproveitamento adequado das funcionalidades da nova plataforma.
- 3.5.2. Planejamento da Estratégia de Migração
 - 3.5.2.1. Elaboração de um plano detalhado de migração contendo cronograma, critérios de sucesso, responsáveis, plano de comunicação e fluxos operacionais.
 - 3.5.2.2. Levantamento e análise de todos os repositórios, pipelines, runners, artefatos e configurações da instância atual.
 - 3.5.2.3. Definição de janelas de manutenção e estratégias de fallback (rollback) para mitigação de falhas durante a migração.
 - 3.5.2.4. Aprovação do plano pela equipe técnica da ALESP e validação de checklist pré-migração.
- 3.5.3. Identificação de Riscos e Medidas Mitigadoras
 - 3.5.3.1. Avaliação de riscos operacionais, técnicos e de segurança relacionados à migração.
 - 3.5.3.2. Identificação de pontos críticos, como serviços interdependentes e integrações com ferramentas externas.
 - 3.5.3.3. Proposição de mecanismos de mitigação, incluindo backups completos, checkpoints intermediários e testes de integridade pós-migração.
 - 3.5.3.4. Implementação de plano de contingência documentado.
- 3.5.4. Execução Assistida da Migração
 - 3.5.4.1. Apoio técnico integral durante a execução da migração.
 - 3.5.4.2. Importação dos repositórios Git, histórico de commits, pipelines e configurações existentes.
 - 3.5.4.3. Reconfiguração dos runners de CI/CD e revalidação dos pipelines.
 - 3.5.4.4. Verificação pós-migração: consistência de dados, funcionamento de automações, permissões e rastreabilidade.
- 3.5.5. Integração com Clusters Kubernetes Existentes

- 3.5.5.1. Levantamento da infraestrutura atual de orquestração (Docker Swarm e Kubernetes).
- 3.5.5.2. Mapeamento de serviços e workloads que deverão ser integrados à nova instância GitLab.
- 3.5.5.3. Apoio técnico na configuração do GitLab Kubernetes Agent para conectar ambientes existentes e permitir deploys automatizados e seguros.
- 3.5.5.4. Testes funcionais de integração e validação de fluxos de CI/CD.
- 3.5.6. Apoio à Migração de Repositórios de Artefatos
 - 3.5.6.1. Levantamento de repositórios atuais de artefatos (ex: Docker Registry, Nexus, Maven).
 - 3.5.6.2. Planejamento e execução de migração para GitLab Container Registry, Package Registry e outros repositórios suportados.
 - 3.5.6.3. Reconfiguração dos pipelines para uso das novas referências.
 - 3.5.6.4. Validação do acesso e versionamento dos artefatos migrados.
- 3.5.7. As atividades acima deverão ser executadas de forma assistida pela contratada, em conjunto com a equipe técnica da ALESP, com base em cronograma previamente pactuado, visando garantir a continuidade, segurança e integridade do ambiente durante todo o processo de migração.
- 3.5.8. Volumetria Estimada
 - 3.5.8.1. A instância atual do GitLab da ALESP possui aproximadamente 112Gb GB de dados, incluindo código-fonte, pipelines, histórico e artefatos de build, com crescimento aproximado de 1Gb/mês;
 - 3.5.8.2. Tamanho médio dos repositórios: 60Mb/repositório
 - 3.5.8.3. A volumetria estimada pode sofrer variações da ordem de 30%, considerando expansão natural de dados e novas demandas futuras.
 - 3.5.8.4. A média atual de acessos diários à instância é de 5.000 acessos, podendo atingir picos de 20.000 acessos/dia, o que demanda infraestrutura e planejamento compatíveis para absorção da carga sem interrupções.
 - 3.5.8.5. Número de usuários ativos: 75
 - 3.5.8.6. Número de usuários bloqueados: 89
 - 3.5.8.7. Número de repositórios: 489
 - 3.5.8.8. Execuções de pipelines (dia/mês): 20/dia e 348/mês
 - 3.5.8.9. Quantidade e tipo de runners: 4
 - 3.5.8.10. Complexidade dos pipelines: média
 - 3.5.8.11. Ambientes atendidos: dev/hml/prod

3.6. Consultoria Especializada - DevSecOps, Processos e Gestão

- 3.6.1. A consultoria especializada constitui etapa estratégica da implantação da solução GitLab Ultimate na ALESP, sendo fundamental para orientar a transformação dos processos atuais, promover o alinhamento às melhores práticas de mercado e garantir a evolução da maturidade organizacional no uso de ferramentas de desenvolvimento, segurança e gestão ágil. Esta consultoria será conduzida de forma colaborativa com a equipe técnica da ALESP, respeitando as particularidades institucionais e os objetivos estratégicos de modernização.
- 3.6.2. Diagnóstico de Maturidade
 - 3.6.2.1. Realização de diagnóstico técnico-operacional com base nos modelos GitLab Maturity Assessment e Customer Success Plan (CS Plan);
 - 3.6.2.2. Levantamento de práticas existentes, mapeamento de gaps de maturidade e recomendações de curto, médio e longo prazo;
 - 3.6.2.3. Elaboração de relatório com plano de ação estruturado, incluindo roadmap de evolução institucional com marcos de entrega e priorização de iniciativas.
- 3.6.3. Definição de Processos Baseados em Práticas DevSecOps
 - 3.6.3.1. Estruturação de processos de desenvolvimento seguros e integrados, alinhados às práticas de DevSecOps;
 - 3.6.3.2. Definição de esteiras de CI/CD com validações de segurança (SAST, DAST, SCA, etc.) em múltiplas fases do ciclo de vida;
 - 3.6.3.3. Estabelecimento de fluxos padronizados com gates de aprovação, políticas de merge e padrões de qualidade de código;
 - 3.6.3.4. Orientação para adoção de práticas de shift-left, automação de testes e rastreabilidade de segurança desde o início do ciclo de desenvolvimento.
- 3.6.4. Estruturação da Gestão Ágil de Projetos
 - 3.6.4.1. Implantação de estrutura de gestão ágil no GitLab, com uso de boards, epics, milestones e issues hierarquizadas por valor e complexidade;
 - 3.6.4.2. Capacitação para uso das funcionalidades de planejamento iterativo, backlog, sprints e acompanhamento de entregas;
 - 3.6.4.3. Customização de fluxos de trabalho para diferentes áreas da ALESP (desenvolvimento, infraestrutura, análise de negócios, etc.).

- 3.6.5. Modelagem de Fluxos de Trabalho Personalizados
 - 3.6.5.1. Levantamento dos processos específicos de cada equipe ou unidade da ALESP para modelagem de fluxos personalizados;
 - 3.6.5.2. Implementação de templates de projeto, definições de etiquetas (labels), regras de aprovação e automações por contexto;
 - 3.6.5.3. Implantação de políticas de versionamento, liberação e gestão de mudanças adaptadas às características de cada domínio técnico.
- 3.6.6. Implantação e Análise de Métricas Estratégicas
 - 3.6.6.1. Implantação de métricas estratégicas no GitLab com base nos princípios de Value Stream Management (VSM);
 - 3.6.6.2. Definição e acompanhamento de métricas DORA (Deployment Frequency, Lead Time for Changes, Change Failure Rate, Time to Restore Service);
 - 3.6.6.3. Criação de dashboards para acompanhamento da eficiência, confiabilidade e impacto dos times e projetos;
 - 3.6.6.4. Orientação para uso de indicadores na priorização de ações, identificação de gargalos e avaliação da evolução da maturidade DevOps.
- 3.6.7. A consultoria deverá ser conduzida por profissionais certificados e com experiência comprovada em projetos similares

3.7. Educação e Treinamento

- 3.7.1. A capacitação dos usuários e administradores da plataforma GitLab Ultimate é etapa essencial para assegurar a efetiva apropriação das funcionalidades implantadas, fomentar a autonomia técnica das equipes da ALESP e consolidar a cultura de boas práticas em desenvolvimento, segurança, operações e gestão ágil. O programa de educação e treinamento deverá ser estruturado de forma abrangente, contínua e segmentada, conforme descrito a seguir:
- 3.7.2. Elaboração de Trilhas de Aprendizagem Segmentadas
 - 3.7.2.1. Construção de trilhas de capacitação customizadas por perfil de usuário e área de atuação, considerando as seguintes linhas de especialização:
 - 3.7.2.1.1. Desenvolvimento: Git, pipelines, CI/CD, versionamento, revisão de código;
 - 3.7.2.1.2. Segurança da Informação: práticas DevSecOps, SAST, DAST, compliance, rastreabilidade;
 - 3.7.2.1.3. Infraestrutura: integração com Kubernetes, runners, gestão de ambientes, automações;
 - 3.7.2.1.4. Gestão: planejamento ágil, boards, épicos, milestones, métricas e governança.

- 3.7.3. Desenvolvimento de Materiais Didáticos
 - 3.7.3.1. Produção de conteúdos educacionais em diferentes formatos, incluindo:
 - 3.7.3.1.1. Apresentações técnicas (slides e manuais);
 - 3.7.3.1.2. Vídeos tutoriais demonstrativos com narração e simulação de uso;
 - 3.7.3.1.3. FAQs temáticos e guias rápidos de uso para cada funcionalidade abordada;
 - 3.7.3.1.4. Repositório centralizado com versão digital de todos os materiais.
- 3.7.4. Realização de Treinamentos Presenciais e Remotos
 - 3.7.4.1. Condução de treinamentos por instrutores certificados GitLab e com experiência prática em projetos de DevOps;
 - 3.7.4.2. Execução de turmas presenciais e remotas, com cronograma adaptado à disponibilidade das equipes;
 - 3.7.4.3. Realização de avaliação de aprendizado com emissão de certificado de participação;
 - 3.7.4.4. Disponibilização de gravações das sessões síncronas para posterior acesso.
- 3.7.5. Workshops Interativos com Laboratórios Práticos
 - 3.7.5.1. Planejamento de oficinas práticas focadas em contextos reais da ALESP;
 - 3.7.5.2. Execução de exercícios em ambiente simulado ou de homologação, com suporte ativo do instrutor;
 - 3.7.5.3. Estímulo à experimentação de fluxos completos (code > commit > pipeline > deploy > compliance);
 - 3.7.5.4. Aplicação de dinâmicas de resolução de problemas e troubleshooting.
- 3.7.6. Sessões de Acompanhamento Pós-Treinamento
 - 3.7.6.1. Agendamento de sessões de reforço e acompanhamento técnico após os treinamentos iniciais;
 - 3.7.6.2. Esclarecimento de dúvidas emergentes durante o uso real da plataforma;
 - 3.7.6.3. Identificação de dificuldades ou resistências para adoção plena das funcionalidades;
 - 3.7.6.4. Reforço de conceitos estratégicos e boas práticas em sessões específicas por equipe.
- 3.7.7. O plano de educação deverá ser pactuado com a área técnica da ALESP e executado em ciclos progressivos, garantindo que o conhecimento permaneça disseminado de forma ampla, prática e continuada em toda a organização.

3.8. Operação Assistida

- 3.8.1. A operação assistida tem por objetivo garantir o acompanhamento contínuo da adoção da plataforma GitLab Ultimate nas equipes técnicas da ALESP, assegurando suporte personalizado, amadurecimento progressivo do uso da ferramenta, disseminação das boas práticas e consolidação das rotinas de DevSecOps na instituição. Essa etapa também se configura como elo estratégico entre o processo de implantação, os ciclos de capacitação e a internalização definitiva da nova cultura e modelo operacional.
- 3.8.2. Acompanhamento Contínuo da Adoção
 - 3.8.2.1. Acompanhamento periódico da utilização das funcionalidades do GitLab pelas equipes da ALESP;
 - 3.8.2.2. Análise da aderência aos processos definidos durante a consultoria;
 - 3.8.2.3. Apoio na superação de barreiras técnicas e culturais.
- 3.8.3. Sessões Personalizadas por Perfil de Usuário
 - 3.8.3.1. Planejamento de atendimentos diferenciados conforme o perfil dos usuários:
 - 3.8.3.1.1. Desenvolvedores: pipelines, merge requests, versionamento;
 - 3.8.3.1.2. QA/Segurança: testes automatizados, validação de vulnerabilidades;
 - 3.8.3.1.3. Gestores: planejamento ágil, painéis, indicadores.
- 3.8.4. Produção Contínua de Materiais de Apoio
 - 3.8.4.1. Elaboração e disponibilização de novos conteúdos didáticos conforme surgem dúvidas recorrentes ou mudanças de configuração;
 - 3.8.4.2. Atualização dos repositórios internos de boas práticas, FAQs e guias rápidos.
- 3.8.5. Realização de Workshops Práticos por Cenário
 - 3.8.5.1. Execução de oficinas práticas voltadas para os fluxos reais e contextos específicos das equipes da ALESP;
 - 3.8.5.2. Simulações de rotinas críticas e validação de automações em ambiente controlado.
- 3.8.6. Identificação e Capacitação de Agentes Multiplicadores
 - 3.8.6.1. Seleção de agentes-chave internos (por equipe ou unidade) para atuarem como multiplicadores do conhecimento;
 - 3.8.6.2. Treinamento específico e acompanhamento desses agentes para disseminação local de boas práticas.
- 3.8.7. Estabelecimento de Fórum Interno de Usuários
 - 3.8.7.1. Criação e manutenção de espaço colaborativo interno (comunidade de prática) para troca de experiências, dúvidas e sugestões entre usuários da plataforma;

- 3.8.7.2. Dinamização de encontros periódicos para compartilhamento de aprendizados e inovações.
- 3.8.8. Estruturação de Suporte Técnico Local
 - 3.8.8.1. Disponibilização de canais internos de atendimento e plantões de dúvidas (presenciais ou remotos);
 - 3.8.8.2. Registro e acompanhamento de chamados e pontos de melhoria na operação cotidiana.
- 3.8.9. Coleta de Feedback e Iteração Contínua
 - 3.8.9.1. Estruturação de processo sistemático de coleta de feedback dos usuários da plataforma;
 - 3.8.9.2. Proposição de ajustes em processos, configurações ou automações com base nas percepções reais de uso.
- 3.8.10. Posto de Trabalho Presencial de Especialista DevSecOps
 - 3.8.10.1. Deverá ser alocado, de forma presencial na sede da ALESP, 1 (um) posto de trabalho em tempo integral (full-time) de profissional especializado em DevOps, GitLab, integração com Kubernetes, segurança e CI/CD.
 - 3.8.10.2. Este especialista atuará como ponto focal técnico em parceria com o time técnico da Alesp para:
 - 3.8.10.2.1. Apoiar a sustentação e monitoramento do ambiente GitLab;
 - 3.8.10.2.2. Auxiliar nas decisões de arquitetura e configurações avançadas;
 - 3.8.10.2.3. Conduzir atendimentos técnicos de maior complexidade;
 - 3.8.10.2.4. Suportar a implementação e evolução da esteira DevSecOps institucional;
 - 3.8.10.2.5. Cooperar com as equipes internas na solução de problemas e na definição de boas práticas.
 - 3.8.10.3. Justificativa Técnica e de Gestão
 - 3.8.10.3.1. A presença de um especialista dedicado se justifica pela criticidade do ambiente GitLab na sustentação do ciclo de vida das aplicações da ALESP.
 - 3.8.10.3.2. A natureza distribuída das equipes e a necessidade de integração com múltiplos ambientes (infraestrutura, segurança, gestão, etc.) exigem suporte técnico especializado, com agilidade e domínio pleno da solução.
 - 3.8.10.3.3. Além disso, este profissional atuará como catalisador do amadurecimento técnico da equipe interna, promovendo transferência de conhecimento, autonomia e alinhamento contínuo às boas práticas DevSecOps e às metas estratégicas de transformação digital da Casa.

4. REQUISITOS DA CONTRATAÇÃO

- 4.1. A contratação da subscrição GitLab Ultimate, com implantação em ambiente on-premise, deverá atender a um conjunto abrangente de requisitos funcionais, técnicos, operacionais, legais e de suporte, com vistas a garantir a aderência às necessidades da Assembleia Legislativa do Estado de São Paulo (ALESP) e às melhores práticas em governança de tecnologia da informação e comunicação.
- 4.2. Os requisitos foram identificados a partir do levantamento de necessidades realizado com as áreas usuárias e técnicas, bem como da análise de mercado e da avaliação de boas práticas em soluções DevSecOps. Estão estruturados de forma a garantir que a solução contratada atenda integralmente às diretrizes de segurança da informação, conformidade legal, eficiência operacional e sustentabilidade tecnológica.
- 4.3. Os requisitos estão organizados nos seguintes grupos:
 - 4.3.1. Requisitos Funcionais e de Negócio
 - 4.3.2. Requisitos Técnicos e Tecnológicos
 - 4.3.3. Requisitos de Segurança da Informação
 - 4.3.4. Requisitos de Manutenção e Suporte Técnico
 - 4.3.5. Requisitos de Capacitação (Treinamento)
 - 4.3.6. Requisitos Temporais (de Prazo)
 - 4.3.7. Requisitos Legais e Regulatórios
- 4.4. Cada grupo contempla elementos específicos que devem ser observados tanto na definição da solução quanto na execução contratual, garantindo a efetividade e a vantajosidade da contratação. A seguir, apresenta-se a listagem detalhada dos requisitos.
- 4.5. Requisitos Funcionais e de Negócio**
 - 4.5.1. A solução contratada deverá permitir a gestão integrada do ciclo de vida do desenvolvimento de software, incluindo versionamento, revisão de código, automação de CI/CD, gerenciamento de segurança, planejamento ágil e gestão de artefatos.
 - 4.5.2. A plataforma deverá prover esteiras de automação integradas, ferramentas de planejamento ágil, colaboração em tempo real, gerenciamento de tarefas e integração com IDEs.
 - 4.5.3. A plataforma deverá dispor de funcionalidades nativas para planejamento iterativo, organização de backlog, sprints, epics, milestones e visualização em boards.
 - 4.5.4. O sistema deverá permitir o acompanhamento de métricas estratégicas (DORA, VSM) e geração de relatórios de desempenho e conformidade.

- 4.5.5. A solução deverá oferecer painéis de acompanhamento de métricas, histórico completo de mudanças, controle de qualidade de código e gestão por projetos, epics e milestones.
- 4.5.6. A solução deve possibilitar a implementação de práticas DevSecOps que assegurem rastreabilidade, auditoria, validação de segurança automatizada e conformidade com a LGPD e demais normativos vigentes.

4.6. Requisitos Técnicos e Tecnológicos

- 4.6.1. A solução deverá ser entregue na versão "GitLab Ultimate", com todas as funcionalidades habilitadas, para implantação em ambiente local (on-premise);
- 4.6.2. Deverá suportar integração com infraestrutura baseada em Linux, Docker, Kubernetes e sistemas de autenticação corporativa (LDAP, SAML, OAuth);
- 4.6.3. A plataforma deverá possibilitar a migração assistida da instância atual da ALESP, incluindo código-fonte, pipelines, artefatos e configurações, com apoio técnico especializado.
- 4.6.4. O sistema deverá permitir configuração em ambiente escalável com suporte a alta disponibilidade, balanceamento de carga e monitoramento contínuo.
- 4.6.5. A arquitetura da solução deve permitir expansão modular conforme o crescimento institucional, suporte a múltiplos ambientes e integração com diversas ferramentas.
- 4.6.6. A solução deverá ser implantável em ambiente local, garantindo a compatibilidade com a infraestrutura tecnológica existente na ALESP, com integração aos serviços de rede, autenticação e monitoramento já adotados.
- 4.6.7. Deverá permitir integração com ferramentas de segurança e monitoramento existentes.
- 4.6.8. A solução deve suportar orquestração de fluxos de desenvolvimento com validações em múltiplas fases, deploy automatizado, testes e gestão de ambientes.
- 4.6.9. A plataforma deverá ser compatível com ambientes baseados em VMware, Hyper-V, Proxmox, além de suportar integração com nuvens públicas ou privadas.

4.7. Requisitos de Segurança da Informação

- 4.7.1. A solução deverá oferecer recursos nativos para validação automatizada de segurança em múltiplas fases do ciclo de vida (SAST, DAST, SCA, Secret Detection, etc.);
- 4.7.2. Deverá incluir mecanismos de auditoria, rastreabilidade, logs e controle de acesso granular com base em perfis e permissões;

- 4.7.3. A solução deverá estar em conformidade com as diretrizes da LGPD e demais normativos aplicáveis à administração pública.
- 4.7.4. A solução deve oferecer capacidade para gerenciamento automatizado de vulnerabilidades (SAST, DAST, Secret Detection, Container Scanning, Dependency Scanning, entre outros).
- 4.7.5. Deverá incluir políticas de perfis, permissões granulares, autenticação integrada e autenticação multifator nativa ou via integração.
- 4.7.6. A solução deve permitir a geração de dashboards e relatórios detalhados e em tempo real e exportáveis sobre incidentes e ameaças, com indicadores de segurança.
- 4.7.7. A solução deverá estar em conformidade com padrões como ISO/IEC 27001, NIST, LGPD e políticas internas da ALESP.

4.8. Requisitos de Manutenção e Suporte Técnico

- 4.8.1. A contratada deverá garantir suporte técnico especializado durante todo o período de vigência contratual, com tempo de resposta adequado conforme criticidade.
- 4.8.2. Deverá ser prevista operação assistida com acompanhamento contínuo da adoção, capacitação de usuários e apoio em configuração e troubleshooting;
- 4.8.3. Deverá ser alocado 1 (um) profissional especializado, de forma presencial e em tempo integral na sede da ALESP, conforme perfil detalhado neste Termo de Referência.
- 4.8.4. Devem ser estabelecidos SLAs claros com prazos de resposta e solução para diferentes níveis de severidade.
- 4.8.5. A contratada deverá realizar a atualização assistida e controlada do sistema, com planejamento prévio.
- 4.8.6. Deverá disponibilizar base de conhecimento atualizada e acessível para apoio técnico (documentação técnica, FAQs, artigos de solução e materiais de referência).

4.9. Requisitos de Capacitação

- 4.9.1. A contratada deverá elaborar trilhas de capacitação segmentadas (desenvolvimento, segurança, infraestrutura, gestão);
- 4.9.2. Deverão ser realizados treinamentos presenciais e remotos, com instrutores certificados, workshops interativos e sessões pós-treinamento;
- 4.9.3. Todo material didático deverá ser produzido e entregue em português brasileiro e em formato digital (vídeos, apresentações, FAQs, manuais).

4.10. Requisitos Temporais

- 4.10.1. O período da subscrição será de 24 (vinte e quatro) meses a partir da assinatura do contrato e ativação das licenças;

- 4.10.2. A implantação, migração, capacitação inicial e ativação do suporte técnico presencial deverão ser concluídas em até 90 (noventa) dias contados da assinatura do contrato.
- 4.10.3. A contratada deverá garantir a ativação imediata dos canais de suporte ao final da implantação.
- 4.10.4. Realização de treinamentos iniciais em até 5 dias após implantação.
- 4.10.5. A Operação Assistida deverá ser realizada pelo período de 24 (vinte e quatro) meses.

4.11. Requisitos Legais e Regulatórios

- 4.11.1. A contratação deverá observar integralmente a Lei nº 14.133/2021 e a Instrução Normativa SGD/ME nº 94/2022;
- 4.11.2. As licenças e serviços contratados deverão incluir documentação comprobatória de origem e vínculo com a fabricante (GitLab Inc.);
- 4.11.3. A contratada deverá apresentar declarações de conformidade com a LGPD, política de segurança da informação e ausência de infrações legais impeditivas à contratação com o poder público.
- 4.11.4. A solução deverá observar a Política de Segurança da Informação da ALESP, diretrizes do TCU e normas técnicas nacionais e internacionais vigentes.

4.12. Modelo de Licitação

- 4.12.1. Os serviços objeto da presente contratação caracterizam-se como de natureza comum, tendo em vista que são geralmente oferecidos por diversos fornecedores e são facilmente comparáveis entre si, de modo a permitir a decisão de contratação com base no menor preço, por meio de especificações usuais praticadas no mercado.
- 4.12.2. Em virtude da natureza comum dos serviços pretendidos para a contratação, na qual configura-se uma grande quantidade de fornecedores habilitados no mercado brasileiro, permitindo assim a ampla concorrência, sugere-se a **modalidade pregão**, em sua forma eletrônica, eletrônico e o critério de julgamento das propostas será o de **menor preço global**.
- 4.12.3. O pregão, especialmente na forma eletrônica, é destacado pela Lei 14.133/2021 como uma modalidade preferencial para a aquisição de bens e serviços comuns, e a sua escolha se justifica pela sua eficiência processual, economicidade e pela ampliação da competitividade, permitindo maior transparência e participação de licitantes de diferentes localidades, aproveitando as facilidades tecnológicas.
- 4.12.4. A escolha do critério de julgamento das propostas como menor preço global para este processo de licitação fundamenta-se na nova Lei de Licitações e tem como principal objetivo assegurar a seleção da proposta mais vantajosa para a Administração Pública, promovendo a

economia e eficiência dos recursos públicos. O critério de menor preço global proporciona uma análise objetiva e transparente das propostas, permitindo uma comparação direta e clara dos custos totais apresentados pelos licitantes.

- 4.12.5. Dessa forma, evita-se a fragmentação e a dispersão de custos que podem ocorrer em outros métodos de julgamento, assegurando que todos os elementos do objeto contratual sejam considerados de maneira integral.
- 4.12.6. Além disso, a adoção do menor preço global está em consonância com os princípios da isonomia, competitividade e eficiência administrativa, garantindo igualdade de condições entre os participantes do certame e incentivando a apresentação de propostas mais econômicas e vantajosas para a Administração.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Condições Gerais

- 5.1.1. A contratada será responsável pela entrega integral das licenças, serviços e subsistemas previstos neste Termo de Referência, com a devida compatibilidade técnica, adequação funcional e em conformidade com os cronogramas e prazos estabelecidos.
- 5.1.2. A instalação da solução GitLab Ultimate será realizada em ambiente on-premise, sob responsabilidade da ALESP, sendo obrigação da contratada prestar todo o suporte técnico necessário à sua instalação, configuração e ativação.
- 5.1.3. Todos os serviços previstos (migração, consultoria, capacitação, operação assistida e suporte técnico) deverão ser executados com base em metodologia previamente aprovada pela Administração e mediante cronograma detalhado a ser acordado após a assinatura do contrato.
- 5.1.4. A contratada deverá disponibilizar equipe técnica qualificada, nos perfis exigidos neste Termo de Referência, durante todo o período de execução contratual, incluindo a alocação de um profissional especializado em regime presencial e integral.
- 5.1.5. Deverá ser garantida a integração plena da nova solução com os sistemas, ferramentas, fluxos de trabalho e infraestrutura tecnológica já existentes na ALESP, sem prejuízo às atividades em curso.
- 5.1.6. A contratada deverá assegurar a realização de todas as atividades de forma colaborativa com as equipes técnicas da ALESP, promovendo a transferência de conhecimento, documentação adequada e boas práticas.

- 5.1.7. Todo o suporte técnico prestado deverá ser registrado, rastreável, e atender aos Acordos de Níveis de Serviço (SLAs) definidos, com acompanhamento pela fiscalização contratual.
- 5.1.8. O descumprimento das condições aqui estabelecidas ensejará a aplicação das penalidades previstas em contrato, sem prejuízo das medidas administrativas cabíveis.

5.2. Prazos de Entrega

- 5.2.1. Os prazos definidos estão descritos no item 4.10. Requisitos Temporais deste Termo de Referência.

5.3. Local de prestação dos serviços

- 5.3.1. Sede da CONTRATANTE: Av. Pedro Álvares Cabral, 201 São Paulo · CEP 04097-900

5.4. Garantia

- 5.4.1. Para assegurar o fiel cumprimento das obrigações assumidas, a CONTRATADA deverá apresentar garantia contratual correspondente a 5% (cinco por cento) do valor total do contrato, nos termos do art. 96 da Lei nº 14.133/2021, cuja validade deverá observar os prazos até a lavratura do Termo de Recebimento Definitivo e considerará ainda como base de cálculo:
 - 5.4.1.1. no caso do fornecimento (itens 01, 02, 03, 04 e 05), o valor total estimado dos bens e serviços;
 - 5.4.1.2. no caso dos serviços associados de natureza continuada (item 06), o valor estimado para os 12 (doze) primeiros meses de execução.
- 5.4.2. A garantia a ser ofertada pela contratada deverá assegurar o pleno funcionamento da solução GitLab Ultimate implantada, incluindo a infraestrutura on-premise, as licenças de uso, os serviços de migração, capacitação, consultoria e operação assistida, nos termos estabelecidos neste Termo de Referência.
- 5.4.3. Garantia Técnica de Funcionamento
 - 5.4.3.1. A contratada deverá garantir o funcionamento adequado, ininterrupto e seguro da solução, com base nos níveis de serviço (SLA) pactuados no contrato;
 - 5.4.3.2. Deverá assegurar a correção de eventuais falhas, bugs ou comportamentos inesperados decorrentes da instalação, configuração ou personalização da plataforma;
 - 5.4.3.3. A contratada será responsável pelo suporte técnico e pela pronta atuação em caso de incidentes críticos, garantindo a continuidade operacional da plataforma.
- 5.4.4. Garantia de Atualizações e Correções

- 5.4.4.1. Durante todo o período contratual, a contratada deverá garantir acesso às atualizações oficiais da solução GitLab Ultimate, incluindo patches de segurança, correções e melhorias de desempenho;
- 5.4.4.2. As atualizações deverão ser aplicadas de forma assistida, mediante agendamento prévio e validação com a equipe da ALESP, preservando configurações, dados e customizações realizadas.
- 5.4.5. **Garantia sobre os Serviços Profissionais**
 - 5.4.5.1. Os serviços de migração, consultoria, capacitação e operação assistida deverão ser garantidos quanto à sua execução conforme os cronogramas e requisitos acordados;
 - 5.4.5.2. Eventuais não conformidades ou entregas parciais deverão ser corrigidas ou complementadas sem ônus adicional para a Administração;
 - 5.4.5.3. A garantia abrangerá ainda a reposição ou substituição de profissionais alocados que não atendam aos requisitos mínimos exigidos ou apresentem desempenho insatisfatório.
- 5.4.6. **Garantia da Continuidade Operacional**
 - 5.4.6.1. A contratada deverá implementar mecanismos que assegurem a continuidade da operação da solução em caso de falhas, interrupções planejadas ou emergenciais;
 - 5.4.6.2. Deverá manter rotinas de backup, testes de restauração e práticas de alta disponibilidade para prevenir perdas e garantir o restabelecimento rápido do serviço.
- 5.4.7. **Garantia de Conformidade Legal e de Segurança**
 - 5.4.7.1. A contratada deverá garantir que a solução implantada estará em conformidade com os requisitos legais aplicáveis (Lei nº 14.133/2021, LGPD, IN SGD/ME nº 94/2022) e com as normas de segurança da informação da ALESP;
 - 5.4.7.2. Em caso de alterações normativas durante a vigência do contrato, a contratada deverá adequar os serviços e funcionalidades ofertadas sem custos adicionais, desde que tecnicamente viável e acordado entre as partes.

5.5. Obrigações adicionais da CONTRATADA

- 5.5.1. Dar ciência ao CONTRATANTE, imediatamente e por escrito, de qualquer fato que possa prejudicar a execução dos serviços.
- 5.5.2. Prestar prontamente os esclarecimentos que forem solicitados pelo CONTRATANTE, no prazo máximo de 24 horas da notificação.

- 5.5.3. Assumir todas as despesas relativas a pessoal e quaisquer outros incidentes sobre o objeto a ser contratado, exceto as de responsabilidade exclusiva do CONTRATANTE.

6. MODELO DE GESTÃO DO CONTRATO

- 6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
- 6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila, conforme previsto no art.115, §5º, da Lei Federal n.º 14.133/2021.
- 6.3. As comunicações entre a Alesp e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 6.4. Após a assinatura do contrato ou instrumento equivalente, A Alesp poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.
- 6.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.
- 6.6. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.
- 6.7. A Alesp poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.
- 6.8. A execução do presente Contrato será acompanhada e fiscalizada por meio de uma comissão de, no mínimo, 3 (três) membros, a qual anotarà em registro próprio qualquer ocorrência havida que esteja em desacordo com os termos do Edital, seus Anexos ou deste instrumento contratual, determinando, em decorrência disto, o que for necessário à regularização das falhas observadas.
- 6.9. Identificada qualquer inexecução ou irregularidade, a fiscalização do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a sua correção.

- 6.10. O cronograma detalhado das etapas de trabalho será elaborado em conjunto com a CONTRATADA, no prazo máximo de até 10 (dez) dias úteis contados da assinatura do contrato, devendo contemplar todas as fases do projeto, incluindo implantação, migração, consultoria, capacitação e operação assistida.
- 6.10.1. O cronograma deverá ser formalizado por meio de documento específico, contendo a descrição das atividades, marcos de entrega (milestones), responsáveis, prazos estimados e critérios de aceite, sendo submetido à aprovação formal da CONTRATANTE.
- 6.10.2. Após aprovado, o cronograma passará a integrar o contrato como instrumento vinculante de acompanhamento e fiscalização, podendo ser ajustado mediante justificativa técnica fundamentada e aprovação expressa da CONTRATANTE, sem prejuízo dos prazos globais estabelecidos.
- 6.11. O período de medição dos serviços será realizado entre o primeiro e o último dia de cada mês.
- 6.12. O cronograma físico-financeiro do projeto encontra-se no ANEXO I deste Termo de Referência.

7. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

- 7.1. Os serviços serão aceitos se estiverem em acordo com as especificações do Termo de Referência ou possuírem especificações de qualidade superior.
- 7.2. Os serviços executados serão medidos e atestados até o quinto dia útil do mês subsequente e serão considerados apenas os que forem realizados entre o primeiro e o último dia do mês da medição.
- 7.3. Após a atestação, será emitida a autorização de faturamento para a contratada.
- 7.4. O objeto do contrato será recebido por meio da comissão de fiscalização mencionada no item anterior, da seguinte forma:

I - Com a lavratura de Atestado de Execução de Serviço, em até 03 (três) dias, verificado o pleno e fiel cumprimento a todas as disposições do Termo de Referência e da Proposta Comercial;

II - Com a lavratura de Termo de Recebimento Provisório, em até 03 (três) dias, após a lavratura do último Atestado de Execução de Serviço, desde que tenham sido observadas todas as disposições constantes do Termo de Referência e da Proposta Comercial;

III - Com a lavratura de Termo de Recebimento Definitivo, em até 03 (três) dias, decorrido o prazo de observação, fixado em 30 (trinta) dias,

contado a partir da lavratura do Termo de Recebimento Provisório, desde que persista a qualidade dos bens entregues / serviços executados e sua conformidade com as exigências do Edital e desta Ordem de Execução de Serviço, especialmente as contidas no Termo de Referência e na Proposta Comercial.

- 7.5. O recebimento provisório ou definitivo não exclui a responsabilidade civil da CONTRATADA.
- 7.6. A CONTRATADA fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
- 7.7. A fiscalização não efetuará a atestação da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.
- 7.8. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na Proposta Comercial, sem prejuízo da aplicação das penalidades.
- 7.9. O pagamento será efetuado mediante depósito bancário em conta corrente da CONTRATADA, observadas as seguintes condições:
 - 7.9.1. Apresentação de nota fiscal/fatura acompanhada:
 - 7.9.1.1. do respectivo TERMO DE RECEBIMENTO PROVISÓRIO,
 - 7.9.1.2. da certidão conjunta (negativa de débitos ou positiva com efeitos de negativa) de regularidade de contribuições previdenciárias, de tributos federais e da dívida ativa da União;
 - 7.9.1.3. da certidão de regularidade em face do FGTS;
 - 7.9.1.4. da certidão de regularidade em face de débitos trabalhistas, devidamente atualizadas, se necessário for;
 - 7.9.2. Em 30 (trinta) dias, contados da data de apresentação da nota fiscal/fatura. Caso o dia de pagamento recaia em dia não útil, este será efetuado no primeiro dia útil antecedente, sendo certo que, mesmo nesse caso, manter-se-á, na fatura, o dia de vencimento.
- 7.10. Nas operações internas (fornecedores e prestadores de serviços contribuintes do ICMS no Estado de São Paulo), deverá ser observado, quando da entrega do objeto contratado, a correta emissão da Nota Fiscal, nos termos do Decreto Estadual nº 48.034, de 19 de agosto de 2003.

- 7.11. A adjudicatária que não possuir conta no Banco do Brasil S/A deverá providenciá-la após a adjudicação do objeto, para viabilização dos pagamentos.
- 7.12. O requerimento de pagamento, bem como os documentos de cobrança da CONTRATADA, deverão ser entregues a Divisão de Sistemas e Soluções, localizada no Palácio Nove de Julho, sala nº 330 – telefone (11) 3886-8330, ou via correio eletrônico (e-mail) a ser indicado pela Alesp, em arquivos com extensão .pdf, pesquisáveis.
- 7.13. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 7.14. Havendo atraso no pagamento, sobre o valor devido incidirá correção monetária com base na taxa de variação da UFESP (Unidade Fiscal do Estado de São Paulo), e juros moratórios na razão de 1% (um por cento) ao mês, calculados pro rata tempore, em relação ao atraso verificado

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

- 8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com modo de DISPUTA ABERTO, com adoção do critério de julgamento pelo MENOR PREÇO.
- 8.2. A proposta comercial da licitante deverá ser acompanhada de comprovante de empresa parceira certificada do fabricante da ferramenta GitLab.
- 8.3. Para fins de Habilitação, a licitante deverá apresentar a seguinte documentação:
 - 8.3.1. Habilitação jurídica: aquela constante do edital do Pregão.
 - 8.3.2. Habilitação fiscal, social e trabalhista: aquela constante do edital do Pregão.
 - 8.3.3. Qualificação Econômico-Financeira: aquela constante do edital do Pregão.
 - 8.3.4. Qualificação Técnica: conforme itens a seguir.

8.4. Habilitação Técnica

- 8.4.1. Atestados de capacidade técnica: Para fins de habilitação técnica, a licitante deverá comprovar sua aptidão para desempenho de atividade compatível em características, quantidades e prazos com o objeto da licitação, mediante a apresentação de atestados de capacidade técnica, fornecidos por pessoas jurídicas de direito público ou privado, que comprovem a execução anterior de serviços similares em

características técnicas e de porte equivalente, conforme o disposto no art. 67, §1º, da Lei Federal nº 14.133/2021.

- 8.4.1.1. Conforme as diretrizes estabelecidas pelas Súmulas nº 23 e 24 do Tribunal de Contas do Estado de São Paulo, os atestados apresentados devem referir-se à execução direta, pela licitante, de parcelas de maior relevância técnica ou de valor significativo do objeto contratual, devendo tais parcelas estar expressamente destacadas nos documentos comprobatórios.
- 8.4.1.2. Para os fins desta licitação, consideram-se como parcelas de maior relevância:
 - 8.4.1.2.1. Fornecimento e instalação de licenças GitLab Ultimate (itens 1 e 2 do objeto);
 - 8.4.1.2.2. Assistência à migração do ambiente atual da Alesp para o novo ambiente implantado (item 3 do objeto);
 - 8.4.1.2.3. Consultoria especializada em DevOpsSec (item 4 do objeto)
- 8.4.1.3. Os atestados deverão conter, no mínimo:
 - 8.4.1.3.1. Nome ou razão social da entidade contratante, com CNPJ e endereço;
 - 8.4.1.3.2. Objeto contratado, com descrição clara e detalhada dos serviços prestados, especialmente quanto à compatibilidade com os itens relevantes acima;
 - 8.4.1.3.3. Período de execução contratual;
 - 8.4.1.3.4. Valor total do contrato e, se possível, dos itens individualizados;
 - 8.4.1.3.5. Indicação da regularidade da execução e conclusão dos serviços;
 - 8.4.1.3.6. Assinatura do responsável técnico ou gestor do contrato emitente.
- 8.4.1.4. Empresas participantes que não apresentarem a documentação exigida, de forma completa e correta, serão inabilitadas, sem possibilidade de complementação posterior.
- 8.4.1.5. Não serão aceitos atestados genéricos ou que não identifiquem expressamente as parcelas relevantes do objeto não serão considerados válidos para fins de comprovação da capacidade técnico-operacional exigida neste certame.
- 8.4.1.6. A Alesp poderá, a seu critério, diligenciar a pessoa jurídica de direito público ou privado responsável pela emissão dos atestados de capacidade técnica, visando obter informações complementares sobre o objeto fornecido.

8.4.2. Declaração de Visita Técnica ao local no qual serão realizados os serviços, uma vez que a Licitante deverá verificar todas as condições e características relativas à Alesp, bem como estimar recursos necessários para realização integral do serviço especificado no edital, sendo que deverá respeitar as seguintes características:

- 8.4.2.1. A vistoria técnica é recomendada, mas não obrigatória;
- 8.4.2.2. Realizar vistoria técnica prévia junto ao Departamento de Tecnologia da Informação em dia e hora pré-agendados;
- 8.4.2.3. O agendamento seja feito com antecedência mínima de 03 (três) dias úteis da data desejada e em até 5 (cinco) dias antes da data prevista para oferecimento das propostas, por meio do email dss@al.sp.gov.br.
- 8.4.2.4. A licitante realizará a vistoria prévia mediante o acompanhamento de funcionário indicado pela ALESP.

8.4.3. Declaração de ciência, emitida pela licitante, das condições da documentação verificada na visita técnica, se realizada pela licitante.

8.5. Equipe Técnica

8.5.1. Em face da relevância estratégica da presente contratação e visando garantir a execução segura do contrato, as licitantes deverão apresentar, **para a assinatura do contrato**, profissionais qualificados em seu quadro funcional, mediante apresentação atualizada da ficha funcional, carteira de trabalho e certificado de graduação, conforme os perfis mínimos descritos a seguir.

8.5.1.1. **01 (um) Coordenador Técnico do Projeto**

- 8.5.1.1.1. Nível superior completo em área de TI.
- 8.5.1.1.2. Experiência mínima de 2 anos em coordenação de projetos de implantação de plataformas DevOps em órgãos públicos ou empresas.
- 8.5.1.1.3. Desejável certificação PMP, PMI-ACP ou equivalente.

8.5.1.2. **01 (um) Especialista DevSecOps / GitLab**

- 8.5.1.2.1. Nível superior completo em TI.
- 8.5.1.2.2. Mínimo de 2 anos de experiência com GitLab, CI/CD, DevSecOps e integração com Kubernetes.
- 8.5.1.2.3. Desejável certificação GitLab Certified Professional ou CKA.

8.5.1.3. **01 (um) Arquiteto de Soluções DevOps**

- 8.5.1.3.1. Nível superior completo.
- 8.5.1.3.2. Experiência com integração de plataformas DevOps, infraestrutura como código, automação e segurança.
- 8.5.1.3.3. Conhecimentos em GitOps, Kubernetes, Docker, Ansible, Jenkins e Terraform.

8.5.1.4. 01 (um) Especialista em Segurança da Informação

- 8.5.1.4.1. Nível superior em TI
- 8.5.1.4.2. Especialização ou certificações (CompTIA Security+, ISO 27001, etc.).
- 8.5.1.4.3. Experiência em SAST, DAST, SCA, Secret Detection e políticas de segurança DevOps.
- 8.5.1.5. A comprovação de vínculo profissional pode se dar mediante contrato social, registro na carteira profissional, ficha de empregado ou contrato de trabalho, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços, conforme dispõe a Súmula n.º 25 do TCE-SP.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

- 9.1. O valor estimado da contratação consta do Anexo – Planilha de Preços.
- 9.2. Conforme dispõe o art.25, §7º, da Lei Federal n.º 14.133/2021, os preços contratuais serão reajustados anualmente, em função da data-base do orçamento e a variação do índice indicado no Anexo – Planilha de Preços.
- 9.3. Em atendimento ao disposto no art.18, inciso XI, da Lei Federal n.º 14.133/2021, informamos que o orçamento da licitação, constante do Anexo – Planilha de Preços, não tem caráter sigiloso, sendo divulgado junto com o edital da licitação.

10. ADEQUAÇÃO ORÇAMENTÁRIA

- 10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Alesp.

ANEXO I - Cronograma Físico Financeiro

1. O cronograma físico-financeiro que integra o presente Termo de Referência está estruturado no modelo por etapas para os itens que compõe a implantação, com pagamentos vinculados à entrega e à validação de cada uma das etapas previstas para a implementação da solução.
2. Este modelo tem por finalidade assegurar que os desembolsos financeiros pela Administração Pública estejam diretamente condicionados ao efetivo cumprimento das etapas estabelecidas no planejamento do projeto, promovendo maior controle, segurança e transparência no acompanhamento da execução contratual.
3. Os prazos são em dias corridos, contados a partir do primeiro dia útil subsequente à assinatura do contrato.
4. Cada etapa do cronograma corresponde a um conjunto de entregas mensuráveis e verificáveis, previamente descritas nos itens deste Termo de Referência, de modo que o pagamento à contratada somente será autorizado após:
 - a. Entrega completa dos produtos ou serviços previstos para a respectiva etapa.
 - b. Validação técnica pela equipe de fiscalização da Administração.
 - c. Emissão de termo de aceite formal por parte da contratante.

Itens	Etapas	Prazo Previsto	Percentual de Pagamento
1	Fornecimento das licenças GitLab Ultimate	30	100%
2	Implantação da Plataforma GitLab Ultimate	30	100%
3	Migração	90	100%
4	Consultoria (DevSecOps, Processos, Gestão)	60	50%
		90	50%
5	Treinamento	90	100%
6	Operação Assistida	Faturamento mensal, por 24 (vinte e quatro) meses	

ANEXO II - Planilha de Preços Unitários

Item	Descrição	Unidade	Quantidade	Valor Unitário	Valor do Item
1	Licenças GitLab Ultimate	Licenças	100 (por 24 meses)		
2	Implantação da Plataforma GitLab Ultimate	Serviço	1		
3	Migração	Serviço	1		
4	Consultoria (DevSecOps, Processos, Gestão)	Horas Técnicas	300		
5	Treinamento	Usuário Treinado	50		
6	Operação assistida	Meses	24		



Assinado por : FABIO SANCHES MATOS:14248721899

Data assinatura :12/06/2026 22:54:32

Assinado por : NILSON ROBERTO BRITO DOS SANTOS:13127027885

Data assinatura :15/06/2026 20:17:24