TERMO DE REFERÊNCIA

1. OBJETO

1.1. Registro de Preços para contratação de subscrição de ferramenta de software para realização de análise de qualidade e segurança de código-fonte e dependências durante o desenvolvimento de software, conforme especificações, exigências e prazos constantes deste Termo de Referência

1.2. Farão parte deste Registro de Preços, como órgãos participantes, os Tribunais Regionais Eleitorais – TREs e o Tribunal Superior Eleitoral, que serão responsáveis pelas suas respectivas contratações.

2. JUSTIFICATIVA

2.1 Motivo da contratação

No decorrer do desenvolvimento de software é necessário realizar várias checagens. Além das checagens relacionadas com as funcionalidades esperadas do software, também são avaliadas as questões de infraestrutura, bancos de dados, dentre outros. Contudo, em períodos recentes, uma das preocupações mais recorrentes no desenvolvimento e implementação de software são as referentes aos aspectos de segurança.

Vulnerabilidades em software podem levar desde a um uso inadequado do software, perda de dados, comprometimento dos recursos de infraestrutura, até mesmo ao acesso indevido aos dados e recursos do software em questão e de outros softwares disponíveis no ambiente das empresas e das instituições públicas.

De modo a garantir a qualidade do software sob o ponto de vista técnico, bem como detectar e auxiliar na correção de defeitos (*bugs*) e de construções que podem levar a falhas de segurança, faz-se necessária a análise do software durante o seu desenvolvimento. Ferramentas de análise de qualidade e segurança de código-fonte são utilizadas para verificar a qualidade do software que está em processo de construção, tanto em busca de códigos problemáticos que podem eventualmente levar a *bugs* e comportamentos indesejados, como também localizar falhas no código e/ou nas bibliotecas utilizadas que podem ocasionar em comprometimento dos aspectos de segurança.

2.2. Alinhamento com o Planejamento estratégico

Esta contratação está alinhada ao PDTIC TRE-SP 2021 – 2026 (Aprimorar a Segurança da Informação e a Gestão de Dados e Promover Serviços e Soluções de Infraestrutura e Soluções Corporativas) e à ENSEC- JUD.

2.3. Estudos Preliminares

2.3.1. Os estudos preliminares desta aquisição constam do processo SEI 0060380-47.2022.6.26.8000, documento SEI nº 4808755, e verificaram a existência de soluções de software livre para análise de qualidade e segurança de código-fonte, porém estas não atendem a todos os requisitos necessários, sendo escolhida a contratação de subscrição de ferramenta comercial.
2.3.2. A natureza do objeto é comum no mercado de tecnologia da informação.

2.4. Forma de aquisição e critério de seleção do fornecedor

2.4.1. O objeto está em grupo único.
2.4.1.1 A fundamentação para o parcelamento ou não do objeto da contratação encontra-se pormenorizada em tópico específico dos estudos técnicos preliminares.
2.4.2. A licitação será na modalidade PREGÃO, em sua forma eletrônica. A seleção do fornecedor será feita com base no menor preço global do grupo único.
2.4.3. A Detentora da Ata deverá assinar os Termos de Compromisso de Manutenção de Sigilo (Apêndice B).
2.4.4- Optou-se pelo Sistema de Registro de Preço, consoante o art. 3° do Decreto n° 7.892/2013 pela conveniência de adquirir os produtos com entregas parceladas.

3. ESPECIFICAÇÕES DO OBJETO

3.1. Natureza do objeto: Solução de análise de qualidade e Segurança de código-fonte e dependências durante o desenvolvimento de software

A contratação será realizada em conjunto com os Tribunais Eleitorais e o Tribunal Superior Eleitoral, conforme a descrição dos itens abaixo e unidades de medidas correspondentes.

As quantidades dos itens estão relacionadas no Apêndice A - Quantidade Estimada pelo TRE/SP e Órgãos Participantes e Endereços da Disponibilização da solução.

Grupo	**Item**	**Descrição**	**Unidade**	**Quantidade**	**Preço unitário máximo aceitável**	**Preço total máximo aceitável**
ÚNICO	1	Licença de uso de usuário por subscrição por 24 (vinte e quatro) meses de ferramenta de análise de qualidade e segurança de código-fonte e dependências durante o desenvolvimento de software	USUÁRIO	570	R$ 16.459,31	R$ 9.381.806,70

	2	Instalação e configuração da solução no ambiente do Tribunal	UNIDADE	24	R$ 47.198,00	R$ 1.132.752,00
	3	Treinamento com, no mínimo, 20 horas de carga horária	PESSOA	386	R$ 1.725,89	R$ 666.193,54
PREÇO GLOBAL DO GRUPO ÚNICO (soma dos preços totais dos itens 1, 2 e 3)						R$ 11.180.752,24

3.1.1. A licença da solução é por subscrição e inclui atualização e suporte técnico no período da vigência da subscrição.

3.1.2 A instalação e configuração da ferramenta serão realizadas na infraestrutura local do Tribunal (*on premises*).

Observação: Os códigos e descrições do "CATMAT/CATSER" constantes do Compras.gov.br podem eventualmente divergir da descrição dos itens a serem contratados quanto a especificações e outras características. Neste caso, havendo divergência quanto ao código/descrição do CATMAT/CATSER prevalecerão as especificações detalhadas no Anexo I (Termo de Referência).

3.1.3 Características da solução de análise de qualidade e Segurança de código-fonte e dependências durante o desenvolvimento de software:

3.1.3.1 Integração com a ferramenta de versionamento de código Git utilizada pelo Tribunal.

3.1.3.2 Integração com esteiras de integração contínua (CI) e entrega contínua (CD), para automatizar a análise de código em todas as etapas do processo de desenvolvimento de *software*.

3.1.3.3. Verificação estática de código das aplicações (SAST), com suporte, no mínimo, às linguagens de programação Java, Javascript, PHP, Python, .net, Typescript, Ruby.

3.1.3.4. A solução deve permitir a personalização e criação de regras de análise estática de código.

3.1.3.5. A verificação estática de código deve possuir base de dados de vulnerabilidades interna que deve contemplar, no mínimo, os conjuntos de vulnerabilidades publicamente disponibilizados Common Weakness Enumeration (CWE), Common Vulnerabilites and Exposures (CVE) e OWASP Top 10.

3.1.3.6. A solução deve oferecer atualização da base de dados de vulnerabilidades com frequência mínima trimestral.

3.1.3.7. Sugerir alterações no código fonte e/ou fluxo de dados para correção de

problemas de segurança da informação.

3.1.3.8. Verificação de segurança de dependências utilizadas pelas aplicações (SCA).

3.1.3.9. Verificação dinâmica (DAST) para evitar que a aplicação seja implantada com vulnerabilidades.

3.1.3.10. A solução deverá permitir o gerenciamento de portfólio dos projetos analisados.

3.1.3.11. Gestão de vulnerabilidades, com a apresentação do nível de severidade das vulnerabilidades, bem como sugestão de solução.

3.1.3.12. Gerar relatórios e painéis de controle com a visão geral das aplicações e análises realizadas.

3.1.3.13. Relatório de qualidade de código com a indicação dos trechos de código que necessitam de refinamento e a explicação dos problemas encontrados.

3.1.3.14. Relatórios de segurança, contendo a relação de vulnerabilidades encontradas e com proposta de sugestão de correção das vulnerabilidades.

3.1.3.15. Deverá permitir gerenciamento de alertas de segurança

3.1.3.16. A solução deverá ser executada em ambiente local (on premises), sem que seja necessário encaminhar o código-fonte para um serviço externo e/ou na nuvem.

3.1.3.17. A solução deve integrar-se com IDEs (Ambientes de Desenvolvimento Integrado) para indicar problemas ou débitos técnicos em tempo real aos desenvolvedores.

3.1.3.18. A verificação de dependências (SCA) poderá acessar serviços externos ou na nuvem desde que não encaminhe código-fonte para esses ou outros serviços externos e/ou na nuvem.

3.1.3.19. A solução deverá disponibilizar acesso à base de conhecimento, tanto referente ao seu funcionamento bem como às vulnerabilidades de código por ela reconhecidas.

3.1.3.20. Deve indicar nível de cobertura de testes unitários e configuração de percentagem mínima de aceitação

3.1.3.21 A execução da verificação dinâmica (DAST) poderá ser realizada sequencialmente ou simultaneamente

3.1.3.22 A verificação dinâmica (DAST) deverá permitir o teste dinâmico de aplicações que necessitem de autenticação

3.1.3.23 Deve permitir o agendamento ou execução periódica de análise dinâmica (DAST)

3.2. Instalação e configuração da solução no ambiente do Tribunal

3.2.1. A Detentora da Ata deverá entregar a solução adquirida completamente funcional, dentro das especificações deste Termo de Referência, e dentro do prazo estipulado.

3.3. Treinamento

3.3.1 Serviços de treinamento de no mínimo 20 horas em horário comercial sobre a solução contratada, de forma remota, on-line por videoconferência;

3.3.2 Deverá ser fornecido certificado para cada participante, contendo a respectiva data, carga horária e assinatura do técnico responsável/empresa fornecedora;

3.3.3 Deverá ser do tipo Hands-on para os técnicos designados pelo Órgão Gerenciador/Participante.

3.3.4 Deverão ser demonstradas as principais funcionalidades da solução contratada.

3.3.5 Deverá demonstrar no ambiente instalado os recursos habilitados, configurações realizadas, e outros cenários possíveis para a equipe técnica do Órgão Gerenciador/Participante, explicitando a forma de utilização da solução e de seus recursos;

3.3.6 Deverão ser fornecidos material didático digital, documentação do projeto e manuais de produto.

3.3.7 As atividades serão realizadas em dias úteis e horário compatível com o horário de funcionamento do Tribunal, das 8h às 20h, exceto quando por necessidades do Órgão Gerenciador/Participante, a ser acordado entre as partes.

3.4 – Será(ão) desclassificada(s) a proposta(s) que, após a etapa de negociação, mantiver(em) seu(s) preço(s) unitário(s) superior(es) ao(s) preço(s) unitários máximo(s) aceitável(is) pela Administração.

4. LOCAL DE EXECUÇÃO OU DISPONIBILIZAÇÃO DO SERVIÇO

A execução e a disponibilização das soluções contratadas se darão nos locais indicados no Apêndice A - QUANTIDADE ESTIMADA PELO TRE/SP E ÓRGÃOS PARTICIPANTES E ENDEREÇOS DA DISPONIBILIZAÇÃO DA SOLUÇÃO.

5. PRAZO DE DISPONIBILIZAÇÃO E INÍCIO DA PRESTAÇÃO DO SERVIÇO

5.1. Prazo para disponibilização das licenças (item 1): até 5 (cinco) dias corridos, contados do recebimento da Nota de Empenho.

5.2. Prazo para implantação e configuração da ferramenta na infraestrutura (item 2): até 10 (dez) dias úteis, contados do recebimento da disponibilização das licenças.

5.3. Prazo para o treinamento da ferramenta (item 3): até 30 (trinta) dias corridos, contados do recebimento (ou aceitação) da implantação e configuração da ferramenta.

6. CONDIÇÕES DE RECEBIMENTO

6.1. O recebimento das licenças (item 1) será efetuado provisoriamente por funcionários do quadro de pessoal da Contratante, conforme modelo do Apêndice C, no prazo de até 5 (cinco) dias úteis.
6.2. Após o recebimento provisório das licenças e implantação da solução (item 2), será realizado Teste de funcionamento para verificar o atendimento ao estabelecido nas especificações técnicas descritas neste Termo de Referência.
6.3. O aceite e a inspeção técnica serão efetuados a fim de verificar a conformidade deles com as especificações técnicas dispostas na descrição deste Termo de Referência.
6.4. Considerar-se-á como data efetiva de disponibilização e implantação da solução aquela aposta no Termo de Recebimento Definitivo emitido pela referida Fiscalização (conforme modelo do Apêndice D), que se dará após a conclusão do teste.
6.5. No caso de constatação de não conformidade, a data efetiva de disponibilização e implantação da solução será a da regularização total da(s) pendência(s).
6.6. Do atesto do treinamento (item 3). Considerar-se-á cumprida a obrigação com a emissão de certificado de realização do treinamento, nos moldes do subitem 3.3. deste Termo de Referência.

7. FORMA COMO OS SERVIÇOS SERÃO SOLICITADOS

7.1. A disponibilização e acessos das licenças, implementação da solução e treinamento serão efetuados após o recebimento da Nota de Empenho e assinatura do respectivo contrato, por cada Tribunal.
7.2. O recebimento da Nota de Empenho e a assinatura do respectivo contrato serão formalizados pelas unidades responsáveis de cada Tribunal.
7.3. Durante a vigência da Ata de Registro de Preços, a detentora fica obrigada a entregar a solução de acordo com o preço registrado, nas quantidades indicadas em cada Nota de Empenho e seu respectivo contrato.
7.4. Os tribunais participantes não estão obrigados a contratar a solução cujo preço foi registrado, ficando a seu critério definir a realização, quantitativo e o momento da execução daquele, de acordo com as especificações constantes deste Termo de Referência.
7.5. A Detentora da Ata não poderá, sem motivo justo, devidamente comprovado e informado, recusar-se a executar o serviço solicitado pelo Tribunal participante.

8. FORMALIZAÇÃO DO CONTRATO

8.1. A vigência do contrato será de 24 (vinte e quatro) meses, podendo ser

prorrogado até o limite previsto no art. 57, IV da Lei n° 8.666/1993.
8.2. Não será admitida a subcontratação do objeto.

9. GARANTIA E SUPORTE DO PRODUTO OU SERVIÇO

9.1Garantia
9.1.1. A garantia e suporte terão prazo de 24 (vinte e quatro) meses.

9.1.2. A garantia das licenças e serviços inclui as atualizações da solução e inclusão de novas funcionalidades ou recursos disponibilizados durante a vigência contratual, cujas despesas decorrentes serão de inteira responsabilidade da Detentora da Ata.

9.1.3. O início do prazo da garantia se dará com o aceite definitivo da solução contratada.

9.2. Suporte

9.2.1. O suporte técnico deverá ser remoto, em português, acionável por interface web ou por telefone no Brasil para o esclarecimento de dúvidas referentes à utilização da solução ou para submissão de problemas de funcionamento da solução.
9.2.2. O suporte técnico será acionado pela abertura de chamados técnicos que conterão, além do detalhamento da solicitação de suporte, a indicação do nível de severidade.
9.2.3. O serviço de suporte técnico deverá contemplar a definição de, ao menos, três níveis de severidade, com características e tempos de resolução (definitiva ou de contorno) conforme a tabela abaixo:

Severidade	**Descrição**	**Tempo de Atendimento**
Alta	Solução sem condições de utilização	Até 2 dias úteis
Média	Solução em operação, porém com funcionalidades importantes sem condições de utilização	Até 6 dias úteis
Baixa	Todos os demais problemas ou solicitações de orientação de uso	Até 15 dias úteis

9.2.3.1. Caso a solução apresentada pelo suporte não seja definitiva (solução de contorno), deverá ser apresentado ao Tribunal plano de solução definitiva em até 10 dias úteis.

10. INDICAÇÃO DE PESSOAL

Será(ão) designado(s) pelo Órgão Gerenciador/Participante servidor(es) para fiscalizar e acompanhar a execução do objeto, nos termos do art. 67 da Lei nº 8.666/93 e tudo o que dispõe a presente contratação.

11. OBRIGAÇÕES DA DETENTORA DA ATA DE REGISTRO DE PREÇOS

A Detentora da Ata, sem prejuízo do atendimento à legislação vigente, obriga-se a:

11.1 - executar fielmente o objeto da Ata de Registro de Preços na mais perfeita conformidade com o estabelecido, comunicando imediatamente ao Órgão Gerenciador/Participante, por intermédio da Fiscalização, por escrito, a ocorrência de qualquer fato impeditivo ou relevante à execução do objeto, sem prejuízo de prévia comunicação verbal dos fatos, caso a situação exija imediata providência por parte daquela;

11.2 - indicar, na Proposta Definitiva de Preços, a qualificação (nome e CPF) do preposto que representará a empresa durante a vigência do ajuste. Se houver a substituição desse profissional, a qualificação do novo PREPOSTO deverá ser informada no prazo de 24 (vinte e quatro) horas, por intermédio de correio eletrônico endereçado à equipe de Fiscalização do Órgão Gerenciador/Participante.

11.2.1 - A Detentora da Ata deverá substituir, sempre que exigido pelo Gestor da Ata, o(s) preposto(s) ou técnico(s), cuja qualificação, atuação, permanência ou comportamento forem julgados prejudiciais, inconvenientes ou insatisfatórios às normas da Administração Pública.

11.3 - providenciar, no prazo máximo de 24 (vinte e quatro) horas, a atualização dos números de telefone e o endereço de e-mail, sempre que houver alterações destes;

11.4 - manter durante toda a vigência da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para a contratação, comprovando-as, a qualquer tempo, mediante solicitação do Órgão Gerenciador/Participante;

11.5 - consentir durante a execução do ajuste, que seja realizada Fiscalização, atentando-se para as observações, solicitações e decisões do Fiscal, desde que justificadas, não ficando, contudo, eximida de sua total responsabilidade sobre todos os serviços contratados;

11.6 - responsabilizar-se por danos pessoais ou materiais causados diretamente por

seus funcionários na execução do objeto da Ata, decorrentes de sua culpa ou dolo, apurados após regular processo administrativo;

11.7 - cumprir todas as leis, decretos, regulamentos, portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto da Ata de Registro de Preços, como a Lei Nº 12.527/2011- Lei de Acesso à Informação, a Lei nº 13.709/ 2018 - Lei Geral de Proteção de Dados Pessoais, dentre outras;

11.8 - A Detentora da Ata responderá por quaisquer prejuízos que seus empregados causarem ao patrimônio do Órgão Gerenciador/Participante ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente, apurados após regular procedimento administrativo.

11.9 - A Detentora da Ata arcará com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do ajuste, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.

12. OBRIGAÇÕES DO ÓRGÃO GERENCIADOR/PARTICIPANTE

O Órgão Gerenciador/Participante obriga-se a:

12.1 - promover, por intermédio da Fiscalização, o acompanhamento e a fiscalização dos serviços, sob os aspectos quantitativo e qualitativo, anotando em registro próprio as falhas detectadas, comunicando à Detentora da Ata as ocorrências de quaisquer fatos que exijam medidas corretivas;

12.2 - verificar se durante a vigência da Ata estão sendo mantidas todas as exigências, condições de habilitação e qualificação da Detentora da Ata;

12.3 - efetuar o pagamento à Detentora da Ata, nos termos previstos na cláusula14.

13. DOCUMENTAÇÃO TÉCNICA DA LICITANTE

13.1. A licitante deverá apresentar, juntamente com sua proposta eletrônica de preços, declaração que comprove, por documento ou site oficial do fabricante, ser parceiro ou empresa credenciada apta a comercializar os produtos indicados para órgãos públicos.

13.1.1. A exigência justifica-se em razão da complexidade da(s) solução(ões) a ser(em) adquirida(s), bem como pelas condições exigidas pelo mercado para comercialização.

13.1.2 O fabricante poderá ser consultado a validar a compatibilidade dos itens e as declarações apresentadas, de modo a validar as condições de garantia existentes.

14. CONDIÇÕES DE PAGAMENTO

14.1 - Os pagamentos serão realizados pelo Órgão Gerenciador/Participante, de acordo com os prazos e termos abaixo dispostos:
14.1.1 – O pagamento dos itens 1 e 2 serão efetuados pela Seção de Pagamento de Contratos e Diárias, por ordem bancária, até o 10º dia útil após a regular prestação dos serviços, mediante Termo de Recebimento Definitivo (modelo constante do Apêndice D deste Termo de Referência), acompanhado da correspondente nota fiscal/fatura, considerando-se como data de pagamento o dia da emissão da ordem bancária, mediante crédito em nome da contratada, em instituição financeira por ela indicada.
14.1.2. O pagamento do item 3 será feito até o 10º dia útil, à vista da emissão dos respectivos certificados de realização de treinamento.

15. DA ATA DE REGISTRO DE PREÇOS

15.1. A Ata de Registro de Preços vigorará pelo prazo de 12 (doze) meses, contados a partir da data da assinatura do documento pela Adjudicatária.
15.2. A Ata de registro de Preços deverá ser firmada dentro do prazo de validade da proposta.

15.3. O preço registrado é fixo e irreajustável durante a vigência da Ata de Registro de Preços, salvo o disposto nos artigos 17 a 19 do Decreto nº 7.892/2013.

16. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

16.1 - Nos termos do art. 67 da Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a execução do objeto, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.
16.2 - A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Detentora da Ata, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.
16.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução da Ata de Registro de Preços, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

APÊNDICE B

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

O TRIBUNAL xxxxxx, CNPJ xxxxxx, sediado Rua xxxx, n° xxx, Bairro xxxx, em xxxxx – CEP: xxxxxx,

OU

TRIBUNAL SUPERIOR

ELEITORAL OU
TRIBUNAL REGIONAL ELEITORAL DO ESTADO DE

doravante denominado CONTRATANTE, e, de outro lado, a «NOME DA EMPRESA> sediada em
«ENDEREÇO, CNPJ NP «CNPJ>, doravante denominada CONTRATADA.

CONSIDERANDO que, em razão do CONTRATO XXXXXX, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação dessas informações sigilosas, bem como definir as regras para seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Comunicação do TRE-SP disponível no sítio do TRE-SP da Internet (www.tre-sp.jus.br);

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula primeira — DO OBJETO
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações disponibilizadas pelo CONTRATANTE, bem como para cumprimento da Política de Segurança da Informação e Comunicação do TRE-SP, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 7.845 de 14/112012 — Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda — DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com os procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.