Estudos Preliminares

Tribunal Regional Eleitoral de São Paulo
Estudos Preliminares - v. 2.2

1 – Identificação do Estudo Preliminar

Este estudo tem por finalidade atender à Estratégia de Cibersegurança da Justiça eleitoral com a contratação por subscrição de software para realização de análise de qualidade e segurança de código-fonte e dependências durante o desenvolvimento de software, conforme a definição de requisitos destes Estudos Preliminares, incluindo serviços de implantação da solução, treinamento, atualização e suporte.

A contratação será realizada em conjunto com os Tribunais Regionais Eleitorais que estiverem interessados na participação, sendo que a licitação deverá ser realizada pelo Tribunal Regional Eleitoral de São Paulo (TRE-SP).

2 – Análise de Viabilidade da Contratação

2.1 – Definição e a especificação dos requisitos

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.

Dentre as principais verificações presentes em ferramentas de análise de qualidade e segurança de código-fonte e dependências, podemos destacar as seguintes:

- Análise Estática de Código-Fonte (*Static Analysis Software Testing* ou SAST): consiste na análise do código-fonte do software, realizada sem que o software em questão esteja em execução, tem por finalidade localizar falhas de segurança no código enquanto ele está sendo escrito pelos desenvolvedores;
- Análise Dinâmica de Software (*Dynamic Analysis Software Testing* ou DAST): trata-se da análise do software em execução, com a simulação de operações no software comumente realizadas por *hackers* em busca de vulnerabilidades. É uma análise do tipo "caixa-preta", que busca vulnerabilidades baseadas em operações específicas e não-triviais que levam a utilização inadequada do software;
- Análise de Composição de Software (*Software Composition Analysis ou SCA*): para construir um software normalmente são utilizados componentes e bibliotecas. Uma

análise de composição de software tem por finalidade elencar as dependências em termos de componentes e bibliotecas, verificar se tais dependências estão atualizadas ou com alguma vulnerabilidade de segurança. Por fim, a análise de composição de software busca garantir que a origem das bibliotecas esteja íntegra;

- Análise Interativa de Software (*Interactive Analysis Software Testing* ou IAST): a análise interativa de software busca combinar elementos da análise dinâmica - verificação do software em execução - com elementos da análise estática. Para tanto faz uso de agentes integrados ao software em análise para obtenção de informações adicionais que irão enriquecer a verificação e análise.

A utilização das verificações elencadas de forma isolada ou em conjunto apresenta-se como fundamental para garantir a qualidade do software desenvolvido face às crescentes ações tomadas por usuários maliciosos e *hackers* com o intuito de comprometer os serviços oferecidos e até mesmo a nossa imagem institucional.

A contratação visa atender às necessidades de vários Tribunais Regionais Eleitorais, bem como do c. Tribunal Superior Eleitoral. Foi realizada uma consulta inicial com cada Tribunal, com a finalidade de buscar um entendimento das necessidades e particularidades de cada um, com a identificação do cenário seguinte:

- Um tribunal utiliza a ferramenta Sonarqube na sua modalidade de código-aberto para análise estática SAST
- Outro tribunal adquiriu e utiliza a ferramenta Tenable somente para análise dinâmica DAST, bem como utiliza a ferramenta de código aberto dependency-check para análise de dependências (SCA)
- Os demais tribunais que responderam a pesquisa não possuem ferramentas de análise de código-fonte

2.1.1 Definição

Para realizar as verificações elencadas no item 2.1, podemos identificar duas soluções possíveis:

Solução 1 - Utilizar ferramentas de código aberto como, por exemplo, as seguintes:

a) Gitlab Community Edition
b) Sonarqube Community Edition
c) OWASP ZAP
d) OWASP Dependency Check

Solução 2 - Utilizar ferramentas comerciais disponíveis no mercado de TIC. Por exemplo, podemos identificar as ferramentas abaixo:

GitLab Ultimate	
Características	**Fornecedores**
Análise dinâmica do tipo DAST (Dynamic Application Security Testing) Dashboards de segurança Gerenciamento de vulnerabilidades Análise de dependências Análise de container Análise estática do tipo SAST (Static Application Security Testing) Mais informações: https://about.gitlab.com/pricing/ultimate/#wu-ultimate-features	GitLab: https://about.gitlab.com/sales/ Ig Corporate: https://www.igcorporate.com.br/contato/ Just Software: GitLab sales: https://www.justsoftware.com.br/contato.html
Fortify On Demand	

Características	Fornecedores
Avaliações estáticas de segurança de aplicações – SAST e Fortify Static Code Analyzer (SCA) Avaliações de composição de OSS Avaliações dinâmicas de segurança de aplicações Web – DAST Teste interativo de segurança de aplicações (IAST) Monitoramento contínuo de aplicações de produção Avaliação dinâmica de segurança de APIs Avaliações de segurança de aplicações móveis Os serviços de teste de segurança de aplicações estáticas, dinâmicas e móveis do Fortify on Demand estão disponíveis por meio da compra e do resgate de unidades de avaliação. Mais informações: https://www.microfocus.com/pt-br/media/data-sheet/fortify-on-demand-ds-pb.pdf	CyberRes: https://www.microfocus.com/pt-br/products/application-security-testing/contact
SonarQube Enterprise	
Características	**Fornecedores**
SonarLint IDE integration SonarQube Análise de ramificações (Branch) Análise de Pull Request Análise de código malicioso (Taint analysis) Processamento paralelo de relatórios de análise Múltiplas instâncias de plataforma de DevOps Customização de regras de segurança Relatórios de segurança Gerenciamento de portfólio e relatórios de execução Relatórios de projeto Logs de auditoria Transferência de projeto Observação: não contempla análise dinâmica (DAST) Mais informações: https://www.sonarsource.com/plans-and-pricing/	SonarSource: https://www.sonarsource.com/company/contact/
HCL AppScan Enterprise	
Características	**Fornecedores**
Análise estática (SAST) Análise dinâmica (DAST) Análise IAST (Interactive Application Security Testing) Controle centralizado e ambiente escalável Relatórios detalhados e dashboards Mais informações: https://www.hcltechsw.com/appscan/offerings/enterprise	HCL Software: https://www.hcltechsw.com/appscan/contact-us OSB Software: https://osbsoftware.com.br/produto/hcl-appscan

2.1.1.1 Contratações similares realizados por outros órgãos

Exército Brasileiro: Contratação de Solução de Análise de vulnerabilidades em Aplicações Computacionais realizada pelo Centro de Desenvolvimento de Sistemas do Departamento de Ciência e Tecnologia. Processo Administrativo nº 64202.011204/2021-15, contrato de 24 meses, 1 licença perpétua para 50 usuários, atualização de licença para mais 10 usuários, treinamento para no mínimo 12 usuários, valor total de R$ 999.062,00.

https://www.citex.eb.mil.br/arquivos/licitacoes/2021/Pregoes/PREGAO%2008_2021-CITEx%20%20(FORTIFY%20-%20CDS)/64202.011204.2021-15.DIGITALIZA%C3%87%C3%83O.%20VOL%204%20Fls%20%20601%20a%20706.pdf

Conselho da Justiça Federal: Contratação de subscrição de ferramenta de gerenciamento de ciclo de vida de software, GitLab, VERSÃO ULTIMATE, por 12 (doze) meses, mediante condições estabelecidas no edital. Contrato de subscrição para 41 licenças, valor total de R$ 264.787,84.

https://www.cjf.jus.br/cjf/transparencia-publica-1/licitacoes-e-contratos/editais/2022/cjf-app-pregao-9

Força Aérea Brasileira: Aquisição de material de Licença perpétua HCL appscan e renovação da garantia e suporte do hcl appscan standard. Nº Processo: 67284004586/2020-75, Licença Perpétua HCL AppScan Standard para 1 (um) usuário com garantia e suporte por 12 (doze) meses e renovação da garantia e suporte do HCL AppScan Standard para 1 (um) usuário por 12 (doze) meses, valor total de R$ 294.800,00

https://www2.fab.mil.br/licitacoesecontratos/index.php/gap-br/3678-pregao-48-2021-aquisicao-de-licenca-perpetua-hcl-appscan-standard

Tribunal Superior Eleitoral: Registro de preços para eventual aquisição de licença perpétua de uso de software para teste e análise estática de segurança de códigos em softwares e aplicações (sistemas informatizados), Pregão Eletrônico 146149/2018, Licitação 58/2021, Solução vencedora Micro Focus Fortify, ata de registro de preços contemplando no mínimo 25 projetos de desenvolvimento, máximo de 200 projetos, 1 licença perpétua de console central de gerência, 1 licença perpétua de serviços de *scanner*, instalação e configuração, repasse de conhecimento e operação assistida. Valor total R$ 2.404.660,63

https://silic.tse.jus.br/silic/pages/internet/licitacao/licitacoes-concluidas.faces

2.1.2 Especificação de Requisitos:

1. Integração com a ferramenta de versionamento de código Git utilizada pelo Tribunal
2. Integração com esteiras de integração contínua (CI) e entrega contínua (CD), que possibilitem a utilização da ferramenta no decorrer do desenvolvimento e entrega dos softwares de forma automatizada
3. Verificação estática de código das aplicações (SAST), com suporte, no mínimo, às linguagens de programação Java, Javascript, PHP, Python, .net, Typescript, Ruby
4. 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
5. A solução deve oferecer atualização da base de dados de vulnerabilidades com frequência mínima trimestral
6. Sugerir alterações no código fonte e/ou fluxo de dados para correção de problemas de segurança da informação
7. Verificação de segurança de dependências utilizadas pelas aplicações (SCA)
8. Verificação dinâmica (DAST) para evitar que a aplicação seja implantada com vulnerabilidades
9. Verificação interativa (IAST) para verificação avançada das aplicações, combinando a análise dinâmica com agentes incorporados no software

10. Gestão de vulnerabilidades, com a apresentação do nível de severidade das vulnerabilidades, bem como sugestão de solução
11. Relatórios de segurança
12. Relatório de qualidade de código
13. Dashboard com a visão geral das aplicações verificadas
14. 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
15. 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

2.2 – Identificação das diferentes Soluções de Tecnologia da Informação e Comunicação

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no portal do Software Público Brasileiro? (http://www.softwarepublico.gov.br)	Solução 1		X	
	Solução 2		X	
Solução é composta por software livre ou software público?	Solução 1	X		
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	Solução 1			X
	Solução 2			X

2.3 – Análise e a comparação entre os custos totais das Soluções de Tecnologia da Informação e Comunicação identificadas

As diversas ferramentas elencadas na Solução 2 possuem formas de licenciamento distintas. De forma geral, as soluções são licenciadas pela quantidade de usuários. Considerando-se a utilização da solução neste Tribunal seriam necessárias 30 (trinta) licenças.

Uma outra métrica utilizada por algumas ferramentas (Sonarqube Enterprise por exemplo) é a quantidade de linhas de código (*Lines of Code* ou LOC). Considerando a realidade dos sistemas desenvolvidos e mantidos no Tribunal seria necessário licenciar 1 milhão de linhas de código. Por fim, algumas soluções de vulnerabilidade de software são licenciadas pelo número de

projetos. Nesse modelo de licenciamento seria necessária uma licença que contemple, no mínimo, 50 projetos considerando os projetos mantidos pelo Tribunal.

As métricas e modelos de licenciamento mencionados podem ser eventualmente combinados de acordo com a ferramenta, o que faz a comparação entre ferramentas ser mais complexa. Desta forma, para efeitos de análise do custo total de propriedade (TCO), devemos considerar quais métricas se aplicam para a realidade do Tribunal e, com base nessas métricas, relacionar as soluções que atendam aos requisitos mínimos elencados mesmo que utilizem métricas distintas.

Finalmente, em relação ao tipo de licença a ser utilizada, a licença perpétua possui como vantagem a possibilidade de utilização da solução mesmo após o término do contrato de suporte. Porém essa vantagem para esse tipo de solução pode se tornar problemática porque soluções de análise de vulnerabilidade - como qualquer solução relacionada com segurança da informação - dependem de atualizações constantes face às ações de *hackers* e demais invasores. Um contrato por subscrição acaba sendo mais vantajoso na medida em que as atualizações e o suporte são mantidos enquanto a subscrição estiver vigente.

Pesquisa inicial para estimativa de valores

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R$	VALOR TOTAL R$
1	Solução de Análise de Vulnerabilidade de Software Gitlab Ultimate licença por subscrição suporte e garantia por 24 meses	30	R$ 30.364,24	R$ 910.927,20
2	Serviços de Instalação e Configuração	1		
3	Treinamento para uso da solução com, pelo menos, 20 horas	30		
			Total	

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R$	VALOR TOTAL R$
1	Solução de Análise de Vulnerabilidade de Software Fortify licença por subscrição suporte e garantia por 24 meses.	30	R$ 45.857,88	R$ 1.375.736,48
2	Serviços de Instalação e Configuração	1	R$ 281.000,00	R$ 281.000,00
3	Treinamento para uso da solução com, pelo menos, 20 horas	30	R$ 2.000,00	R$ 60.000,00
			Total	R$ 1.716.736,48

Item	DESCRIÇÃO DOS PRODUTOS E SERVIÇOS	QTD	VALOR UNIT. R$	VALOR TOTAL R$
1	Solução de Análise de Vulnerabilidade de Software Parasoft licença por subscrição suporte e garantia por 24 meses	30	R$ 14.176,20	R$ 425.286,00
2	Serviços de Instalação e Configuração	1	R$ 87.600,00	R$ 87.600,00
3	Treinamento para uso da solução com, pelo menos, 20 horas	30	R$ 340,00	R$ 10.200,00
			Total	R$ 523.086,00

2.4 – Escolha da Solução de Tecnologia da Informação e Comunicação e justificativa

A demanda tratada nestes Estudos Preliminares é a de uma solução que possibilite a análise de vulnerabilidades de software que possa ser integrada ao processo de desenvolvimento, incorporando questões de qualidade de código-fonte e segurança.

Considerando que as soluções apresentadas previamente atendem ao que foi demandado no Documento de Oficialização da Demanda, não é necessário restringir a contratação para uma ferramenta específica. Entretanto a ferramenta deve preencher os seguintes requisitos:

- Integração com a ferramenta de versionamento de código Git utilizada pelo Tribunal
- Integração com esteiras de integração contínua (CI) e entrega contínua (CD), que possibilitem a utilização da ferramenta no decorrer do desenvolvimento e entrega dos softwares de forma automatizada
- Verificação estática de código das aplicações (SAST), com suporte, no mínimo, às linguagens de programação Java, Javascript, PHP, Python, .net, Typescript, Ruby
- 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
- A solução deve oferecer atualização da base de dados de vulnerabilidades com frequência mínima trimestral
- Sugerir alterações no código fonte e/ou fluxo de dados para correção de problemas de segurança da informação
- Verificação de segurança de dependências utilizadas pelas aplicações (SCA)
- Verificação dinâmica (DAST) para evitar que a aplicação seja implantada com vulnerabilidades
- Verificação interativa (IAST) para verificação avançada das aplicações, combinando a análise dinâmica com agentes incorporados no software
- Gestão de vulnerabilidades, com a apresentação do nível de severidade das vulnerabilidades, bem como sugestão de solução
- Relatórios de segurança
- Relatório de qualidade de código
- Dashboard com a visão geral das aplicações verificadas
- 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
- 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

A ferramenta Sonarqube Enterprise não se aplica a este projeto por contemplar apenas a análise estática de código (SAST), não realizando análise dinâmica de software (DAST).

A solução 1 (ferramentas de código aberto) também não se aplica a este projeto pois, apesar de contemplar alguns dos requisitos técnicos, não implementa diversos requisitos fundamentais para a plena implementação da solução, tampouco conta com suporte técnico dedicado, o que leva a depender de eventual suporte realizado pela comunidade de usuários.

Uma observação importante referente a solução tratada nestes Estudos Técnicos Preliminares é que ela não se confunde com a solução de análise de vulnerabilidades de software a ser licitada pela Seção de Segurança Cibernética (SESEC) por duas razões. Em primeiro lugar, a solução a ser licitada pela SESEC irá contemplar outros softwares que não fazem parte deste projeto, como sistemas operacionais e softwares que compõem o ambiente das estações de trabalho dos servidores, realizando uma análise em vários aspectos distinta da análise realizada pela solução tratada nestes Estudos Técnicos Preliminares. Além disso, a solução aqui proposta é utilizada durante o desenvolvimento de software pelas equipes técnicas deste Tribunal, e não é possível utilizar essa solução para atender as demandas da Seção de Segurança Cibernética e vice-versa.

Portanto a solução escolhida é a solução 2, uma ferramenta comercial de análise de código, que contemple os requisitos elencados e um suporte com nível de serviço compatível com a necessidade do Tribunal.

2.5 – Avaliação das necessidades de adequação do ambiente do órgão para viabilizar a execução contratual

Por se tratar de solução tecnológica, as necessidades de adequação de ambiente do órgão se restringem aos aspectos tecnológicos, em particular de infraestrutura de servidores e armazenamento local considerando-se que a solução será instalada em nosso ambiente (*on premises*). Haverá também ajustes em certos procedimentos e práticas realizadas pela área técnica com a finalidade de incorporar a utilização da solução no processo de desenvolvimento de software.

3 – Sustentação do Contrato

3.1 – Recursos materiais e humanos

Em relação aos recursos materiais, para o objeto em questão se faz necessária uma infraestrutura de rede e de servidores que comporte a execução da solução e sua integração com as demais ferramentas de desenvolvimento e entrega de software utilizados no Tribunal.

Por outro lado, em termos de recursos humanos, a execução do contrato deverá contar com pessoal do Tribunal das seções de Infraestrutura, Gestão de Aplicações, Desenvolvimento e Arquitetura de Sistemas, bem como de funcionários da empresa vencedora da licitação.

3.2 – Continuidade do fornecimento da Solução de Tecnologia da Informação e Comunicação

De modo a garantir a continuidade do fornecimento da solução em caso de eventual interrupção contratual, podemos elencar as seguintes medidas:

- A utilização, de forma paliativa, de ferramentas de código aberto, até que a contratação de uma nova solução seja realizada. O uso de ferramentas de código aberto não possui o mesmo nível de suporte técnico de soluções contratadas. Ademais, tais ferramentas não possuem a mesma gama de recursos e as mesmas atualizações presentes em soluções contratadas;
- Colocar como requisito da solução a aderência a padrões operacionais abertos e de mercado, que possibilitam a mudança de fornecedor de solução ou mesmo da solução em si sem grandes custos no processo de transição de uma solução para outra;

3.3 – Atividades de transição contratual e de encerramento do contrato

Quando do encerramento do contrato, a solução deve possibilitar a exportação das configurações e parâmetros para um formato que permita a aplicação dessas configurações em

outra solução a ser adotada. Além disso, deve ser possível a visualização, consulta e exportação dos logs de verificação realizados pela solução.

3.4 – Regras para estratégia de independência do órgão com relação à empresa contratada

A independência do órgão em relação à empresa contratada se dará pela adoção de padrões abertos de operacionalização, pela manutenção da propriedade do software desenvolvido no TRE-SP que será objeto de análise de vulnerabilidade pela solução, pela capacidade de exportar as configurações em um formato que possibilite a configuração em outra solução a ser adotada.

4 – Estratégia para a Contratação

4.1 – Natureza do objeto

Solução de Análise de Vulnerabilidade de Software.

O objeto possui características comuns e é fornecido usualmente pelo mercado.

Por tratar-se de solução a ser instalada localmente (*on premises*), acompanha serviço de atualização da solução e serviço de suporte e manutenção, sendo um serviço continuado tanto para licença perpétua como para contrato de subscrição, a vigência será de 24 meses, com possibilidade de prorrogação pelo período legal.

Alinhamento Estratégico

Planejamento Estratégico TRE-SP 2021-2026
Macrodesafio:
Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivo Estratégico:
Aprimorar a Segurança da Informação e a Gestão de Dados

4.2 – Parcelamento do objeto com a demonstração da viabilidade ou não da divisão

O objeto será licitado em grupo único.

Não é possível parcelar o objeto uma vez que o produto a ser adquirido é composto por um único software, de natureza indivisível. Eventuais variações em torno da configuração de produtos de mesmo fornecedor são decorrentes do licenciamento para diferentes quantidades de usuários, projetos de software a serem avaliados, e quantidade de linhas de código que compõem tais projetos, que, entretanto, não permitem sua divisão em itens distintos.

Adicionalmente, considerando-se que a aquisição será realizada sem a indicação de marca ou modelo, tem-se que os serviços complementares a serem contratados não podem ser vinculados previamente a nenhum produto específico, mas devem ser vinculados ao produto que venha a ser adquirido, de forma que a separação desses serviços em itens ou lotes distintos também se torna inviável.

Quanto aos serviços de instalação e treinamento, torna-se inviável técnica e economicamente que eles sejam executados por empresas diferentes, uma vez que o domínio sobre a solução e a metodologia de execução dos serviços devem ser tecnicamente compatíveis, e isso só é possível quando a mesma empresa que fornece o software é a mesma que a instale e realize o treinamento.

4.3 – Adjudicação do objeto com a indicação e justificativa da forma escolhida

A adjudicação se dará em grupo único contendo as licenças de uso, a instalação e configuração da solução e o treinamento de uso da solução, pelas razões explícitas no subitem 4.2.

4.4 – Modalidade e o tipo de licitação

Será adotada a modalidade de pregão eletrônico por menor preço, para formação de Ata de Registro de Preços, de modo que o serviço seja prestado conforme a demanda / necessidade de cada Tribunal participante desta aquisição conjunta.

4.5 – Classificação orçamentária e indicação da fonte de recurso

Recursos previstos no orçamento 2023, cuja classificação será oportunamente registrada quando da formalização dos contratos decorrentes das atas de Registro de Preços.

4.6 – Vigência e a indicação do prazo de garantia dos bens e/ou prestação dos serviços contratados

A solução a ser licitada conterá o suporte técnico de 24 (vinte e quatro) meses com possibilidade de renovação do contrato pelo período legal.

4.7 – Equipe de Apoio à Contratação

<inciso VII do Art. 16 da Res. CNJ 182/2013:

Indicar os integrantes da Equipe de Apoio à Contratação, se necessário.>

4.8 – Equipe de Gestão da Contratação

<inciso VIII do Art. 16 da Res. CNJ 182/2013:

Indicar os integrantes da Equipe de Gestão da Contratação (fiscais).>

5 – Análise de Riscos

5.1 – Identificação dos principais riscos

Os principais riscos inerentes a esta contratação são:

1. Licitação deserta
2. Valor ofertado estar acima do estimado na fase de planejamento da contratação
3. Vulnerabilidade de software sendo explorada por não ter sido detectada pela não contratação da solução

5.2 – Mensuração das probabilidades de ocorrência e dos danos potenciais relacionados a cada risco identificado

A probabilidade de ocorrência e os danos de cada risco elencado são:

1. Licitação deserta: risco baixo, com dano provável sendo o atraso na contratação
2. Valor ofertado estar acima do estimado na fase de planejamento da contratação: risco baixo, com dano provável sendo ou o atraso na contratação ou o redimensionamento do objeto
3. Vulnerabilidade de software sendo explorada por não ter sido detectada pela não contratação da solução: risco baixo, com dano provável sendo o esforço adicional em localizar a vulnerabilidade e tratá-la, com gerenciamento do eventual dano à imagem institucional e demais danos relativos aos dados utilizados nos serviços disponibilizados pelo TRE-SP

5.3 – Ações previstas para reduzir ou eliminar as chances de ocorrência

As ações previstas para mitigar, reduzir ou eliminar os riscos elencados são as seguintes:

1. Licitação deserta: contato com fornecedores para avaliação de viabilidade de contratação

2. Valor ofertado estar acima do estimado na fase de planejamento da contratação: contato com fornecedores para avaliação de viabilidade de contratação, pesquisa de contratações semelhantes realizadas por outros órgãos públicos feitas recentemente
3. Vulnerabilidade de software sendo explorada por não ter sido detectada pela não contratação da solução: utilizar soluções de código aberto e buscar apoio na comunidade e em unidades de segurança deste Tribunal e dos demais Tribunais Eleitorais, enquanto temos em vista contratações semelhantes e atas de registro de preço abertas de soluções que atendam a esta demanda.

5.4 – Ações de contingência

Como ações de contingência para os riscos elencados temos:

1. Licitação deserta: acompanhar contratações e atas de registro de preço de soluções semelhantes
2. Valor ofertado estar acima do estimado na fase de planejamento da contratação: acompanhar contratações e atas de registro de preço de soluções semelhantes, propor uma redução do objeto ou a execução em etapas
3. Vulnerabilidade de software sendo explorada por não ter sido detectada pela não contratação da solução: verificações realizadas de forma manual pelos desenvolvedores e pela área técnica responsável pela segurança, bem como o acompanhamento de informes de segurança realizados pelas equipes técnicas enquanto a contratação não é realizada

5.5 – Responsáveis pelas ações de prevenção dos riscos e dos procedimentos de contingência

Item	Risco	Probabilidade de ocorrência	Danos	Ações de mitigação	Responsáveis	Ações de contingência	Responsáveis
1	Licitação deserta	Baixa	Atraso na contratação	Contato com fornecedores	STI, SAM	Acompanhar contratações e atas de registro de preço de soluções semelhantes	STI, SAM
2	Valor ofertado acima do estimado	Baixa	Atraso na contratação Redimensionamento do objeto	Contato com fornecedores Pesquisa em contratações semelhantes recentes	STI, SAM	Acompanhar contratações e atas de registro de preço Propor redução do objeto ou execução em etapas	STI, SAM
3	Vulnerabilidade explorada por não-contratação	Baixa	Esforço adicional em localizar a vulnerabilidade e tratá-la	Utilizar soluções de código aberto e buscar apoio na comunidade e em unidades de segurança deste Tribunal e dos demais Tribunais Eleitorais, enquanto temos em vista contratações semelhantes e atas de registro de	STI, SAM	Verificações realizadas de forma manual Acompanhamento de informes de segurança	STI

				preço abertas de soluções que atendam a esta demanda.			

6 – Declaração de Viabilidade da Contratação

São Paulo, em 26/06/2023.

Diante dos estudos realizados opinamos pela viabilidade da Contratação.

<nome>	<nome>	<nome>
Equipe de Planejamento da Contratação		

Aprovo a viabilidade da Contratação.

<nome>
<Titular da área Demandante>