TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 03/2023 - TRE-ES/PRE/DG/STI/CIS/NSC

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

[Obrigatório mesmo para prorrogações, art. 19, § único, resolução TRE-ES nº 261/2018]

1. CARACTERIZAÇÃO DA DEMANDA

Solução "on premise" de software de análise estática de código e de bibliotecas públicas.

DESCRIÇÃO SUCINTA

Aquisição de licença de software que deverá ser instalada na modalidade “on premise” para a realização da análise estática de código fonte de aplicações e análise das bibliotecas públicas utilizadas nas soluções implantadas na infraestrutura do TRE-ES. Deverá ser contratada a manutenção das atualizações e suporte pelo prazo de 36 meses.

JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

Trata-se de contratação de solução para análise de código prevista na Estratégia Nacional de Cibersegurança da Justiça Eleitoral (processo SEI 0005695-28.2021.6.08.8000), Anexo I - Arquitetura de Ciber Segurança, item SG17 - PID17 - SAST - ANÁLISE ESTÁTICA DE CÓDIGO. E também em atendimento ao item 5.1 da NSI 005 deste TRE-ES que prevê a análise de vulnerabilidades em aplicações implantadas na infraestrutura do TRE-ES.

Atualmente a CSGIT conta com ferramentas gratuitas para a realização da análise de código e de bibliotecas públicas, sendo elas o Sonarqube e o dependency-check, ambas não são as ferramentas mais adequadas para realizar essa tarefa, o Sonarqube é mais voltado para a qualidade do código do que para a análise de vulnerabilidades e o dependency-check não é atualizado com uma frequência satisfatória, podendo demorar muito a detectar problemas em bibliotecas utilizadas nas soluções mantidas pela CSGIT.

O atual foco em segurança demanda que soluções melhores, e mais específicas para a realização da análise de código e de bibliotecas públicas, sejam adquiridas de forma a aumentar a segurança das aplicações ineridas na infraestrutura do TRE-ES, minimizando a probabilidade de um ataque que explore vulnerabilidades que atualmente são desconhecidas e por isso não podem ser tratadas.

Os resultados esperados com a aquisição da solução são:

1) A produção de códigos seguros pela equipe de desenvolvimento da CSGIT, que estará apta à realizar a análise de vulnerabilidades nas soluções e aplicar as correções indicadas.

2) Propiciar uma ferramenta capaz de analisar aplicações de origem externa para análise prévia à implantação na rede local, de forma a impedir que sejam utilizadas, caso não sejam consideradas seguras, após análise de vulnerabilidades.

Dessa forma será possível cumprir os requisitos de análise e parecer técnico estabelecidos pela norma NSI 005 em todas as implantações realizadas na infraestrutura do TRE-ES.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

REQUISITOS RELACIONADOS AO NEGÓCIO

A solução deve prover, no mínimo, os seguintes recursos:

2.1 – Realizar a análise estática de código e análise de bibliotecas públicas, para garantir a segurança das aplicações que serão implantadas na infraestrutura do TRE-ES.

2.2 – Estar atualizada com OWASP top 10, documento padrão de segurança para aplicações que representa um consenso das vulnerabilidades mais críticas para aplicações web.

2.3 – Possibilitar a integração com as ferramentas utilizadas atualmente pela CSGIT, para facilitar o processo de análise do código.

2.4 – Analisar todas as linguagens de programação utilizadas atualmente pela CSGIT, para possibilitar a verificação de toda e qualquer aplicação produzida pela CSGIT ou que venha a ser implantada na infraestrutura do TRE-ES.

2.5 – Fornecer suporte técnico para utilização da solução, para possibilitar máximo aproveitamento da ferramenta.

2.6 – Possuir interface web para gerenciamento da solução, para facilitar a administração da solução.

2.7 – Ser instalada na infraestrutura do TRE-ES

2.8 - Permitir a verificação de código de mais de uma aplicação ao mesmo tempo, para permitir que vários desenvolvedores possam utilizar a ferramenta ao mesmo tempo.

2.9 – Permitir autenticação pelo Active Directory, ferramenta utilizada para autenticação no domínio do TRE-ES.

2.10 – Possuir mecanismos de auditoria, para permitir a verificação do uso da ferramenta.

2.11 – Gerar relatórios com as vulnerabilidades encontradas, para fomentar a confecção de relatórios técnicos sobre a aplicação verificada.

2.12 – Realizar treinamento para repasse de conhecimento da solução, para aumentar a produtividade e utilização da ferramenta.

2.13 – Apresentar o resultado das análises de vulnerabilidades em dashboard configurável pelo administrador da ferramenta, para permitir uma visualização gerencial.

REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

2.14 - Deve haver um treinamento para desenvolvedores e gestores nas funcionalidades da solução.

REQUISITOS DE MANUTENÇÃO E GARANTIA

2.16 - Durante todo o período de contrato deverá ser possível realizar as atualizações da solução.

2.17 – Deverá haver suporte técnico para utilização da solução.

REQUISITOS TEMPORAIS

A solução possuirá atualizações durante o período contratado, após esse período será necessário realizar uma nova contratação para a manutenção das atualizações da solução.

REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

2.19 - Deve ser assinado termo de sigilo e confidencialidade para garantir a segurança física e lógica de todos os documentos, cópias e informações digitais, onde a contratada se compromete a manter em sigilo quaisquer informações de ambiente tecnológico e de negócio da contratante a que tiver acesso durante a realização da instalação ou suporte da solução. O termo de sigilo e confidencialidade deve conter ainda cláusulas específicas que obriguem e estabeleçam prazos para que a contratada, após o término do contrato, elimine todo e qualquer dado pessoal da contratante.

Em relação aos dados pessoais controlados pela CONTRATANTE, esclarecemos que não haverá, no âmbito do CONTRATO, o compartilhamento de dados pessoais ou dados pessoais sensíveis com a CONTRATADA.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

CARACTERÍSTICAS GERAIS

A) Quanto às licenças da solução

3.1. As licenças da solução de software devem ser acompanhadas pelos serviços de suporte técnico remoto pelo fabricante e atualização de versões pelo prazo de, no mínimo, 36 meses.

3.2. A solução de software não deve ter tido sua descontinuidade prevista ou publicada pelo fabricante até o momento da abertura da licitação.

B) Quanto à arquitetura da solução

3.3. Pode ser monolítica ou composta por módulos de sistema de software, desde que sejam do mesmo fabricante, e que se integrem em uma única console de gerenciamento que agregue as funções de administração das configurações da solução e de apresentação das análises de código e análise de bibliotecas públicas.

3.3.1. Será aceita solução em que apenas o módulo para análise de bibliotecas públicas seja *on cloud*, contanto que não haja necessidade de realização de upload do código fonte para a nuvem.

3.4. A console de gerenciamento deve ser acessível via interface Web.

3.5. Deve possuir base de dados de vulnerabilidades interna, que deve contemplar ao menos os três conjuntos de vulnerabilidades publicamente disponibilizados abaixo especificados:

3.5.1. Common Weakness Enumeration (CWE);

3.5.2. Common Vulnerabilities and Exposures (CVE);

3.5.3. OWASP Top 10.

3.6. Deve oferecer atualização da base de dados de vulnerabilidade com frequência mínima trimestral.

3.7. O servidor ou módulo principal (responsável pela gerência da solução) será instalada sobre a infraestrutura de virtualização existente no TRE-ES, implementada sobre o produto VMware 6.0 (ou superior, caso já tenha sido implantada pelo Tribunal).

3.8. O servidor ou módulo principal deve ser instalado sobre um dos sistemas operacionais abaixo relacionados (cujas licenças de uso serão providas pelo Tribunal):

3.8.1. Oracle Linux 8 ou superior;

3.8.2. Microsoft Windows Server 2012 R2 ou Microsoft Windows Server 2019;

3.8.3. Caso os sistemas operacionais acima não sejam compatíveis, a licença de uso do sistema operacional necessário, incluindo os direitos de atualização de versões e suporte técnico deverão ser providas pela

contratada.

3.9. O servidor ou módulo principal deve ser instalado sobre um dos Sistemas Gerenciadores de Banco de Dados (SGBDs) abaixo relacionados:

3.9.1. PostgreSQL 11.13 ou PostgreSQL 13.4 (ou superior, caso a versão já tenha sido atualizada pelo TRE-ES)

3.9.2. Oracle Database 18C (ou superior, caso a versão já tenha sido atualizada pelo TRE-ES);

3.10. Deve incluir as licenças de uso, incluindo os direitos de atualização de versões e suporte técnico remoto prestado pelo fabricante, de todos os demais softwares comerciais necessários à sua instalação e pleno funcionamento.

3.11. Deve permitir a autenticação de seus usuários a partir do Microsoft Active Directory (AD).

3.12. Deve permitir a configuração de perfis de usuários com permissões específicas, para administração da ferramenta, gerenciamento de aplicações cadastradas para avaliação pela ferramenta, submissão de códigos fonte para avaliação pela ferramenta e o respectivo acompanhamento da avaliação, e consulta.

3.13. Deve possuir mecanismos de auditoria que permitam identificar eventos que envolvam: autenticação de usuários, gerenciamento de usuários, de regras de varredura e das varreduras realizadas.

3.14. Deve ser fornecida com todos os recursos necessários para integração com as ferramentas abaixo relacionadas:

3.14.1. Jenkins versão 2 e superior: deve permitir a comunicação bidirecional por meio de plugin e construção de pontos de barreira (threshold) no processo de construção (build);

3.14.2. GitLab versão 14 e superior: deve ser capaz de obter o código fonte para análise a partir do GitLab; deve prover serviço web que permitam a execução automática de varreduras por meio do acionamento de webhooks do GitLab ou por intermédio do Jenkins;

3.14.3. Softwares de gerenciamento de tickets: possibilitar o acionamento de webservices via tecnologia REST para abertura e atualização de tickets no Jira.

3.14.4. Web APIs: Deve disponibilizar APIs REST que possibilitem no mínimo a visualização das regras de análise e dos resultados de varredura.

3.15. Deve permitir a adição de pacote de expansão de uso da solução, seja com base em quantidade de usuários, de projetos, de linhas de código, ou de módulos adicionais, de acordo com o modelo de negócios do fabricante ou da arquitetura da solução.

3.16. A solução deve ser capaz de realizar mais de uma análise em paralelo, sendo que o resultado obtido deve ser o mesmo de análises executadas sequencialmente.

C) Quanto às funcionalidades técnicas

3.17. Deve ser fornecida com capacidade de analisar o código fonte de aplicações em busca de vulnerabilidades de segurança para, no mínimo, as seguintes linguagens de programação, linguagens de marcação e frameworks:

3.17.1. Java 11 com retrocompatibilidade até Java 6;

3.17.2. JSP, JSF, Angular, VUE.js;

3.17.3. Javascript, Typescript;

3.17.4. PHP versões: 5, 7 e superiores;

3.17.5. XML;

3.17.6. HTML;

3.17.7. PL/SQL

3.17.8. Python;

3.17.9. Mobile (Android e IOS);

3.17.10. C#

3.17.11. Asp.net

3.17.12. Docker (dockerfile)

3.18. Deve implementar ao menos as seguintes técnicas de análise:

3.18.1. Buffer: detectar vulnerabilidades de “buffer overflow”, que envolvam a leitura ou escrita do que o buffer pode gerenciar;

3.18.2. Configuração: detectar problemas de segurança em arquivos de configuração das aplicações;

3.18.3. Conteúdo: detectar problemas de segurança em conteúdo HTML estático e dinâmico;

3.18.4. Estrutural: detectar falhas na estrutura ou definição do programa;

3.18.5. Fluxo de Controle: detectar sequências de operações potencialmente vulneráveis;

3.18.6. Fluxo de Dados: detectar potenciais vulnerabilidades referentes à entrada de dados e à posterior utilização desses dados em operações que ofereçam risco;

3.18.7. Semântica: detectar utilização de funções e APIs de forma potencialmente vulnerável;

3.19. As análises de vulnerabilidades devem poder ser realizadas por submissão direta na plataforma e por meio da solução de integração contínua especificados no item 3.14.1.

3.20. Deve possuir uma interface de linha de comando (CLI), que permita a submissão de análises em projetos analisados previamente ou não na ferramenta.

3.21. Deve permitir a visualização em tempo real do status das varreduras em execução.

3.22. Deve permitir ao usuário criar políticas de regras personalizadas que especifiquem quais testes incluir em uma varredura. Tais personalizações deverão ser armazenadas como modelos de configuração de varreduras reutilizáveis, que incluam todos os parâmetros necessários para a execução.

3.23. Deve permitir a identificação de vulnerabilidades em códigos mal concebidos, ou seja, erros que exponham o sistema a riscos de ataques baseados em fatos identificáveis, tais como, por senhas armazenadas de forma não apropriada.

3.24. Deve permitir a indicação de falso-positivos (detecção errônea de vulnerabilidades) e a inclusão de comentários referentes às vulnerabilidades encontradas, mantendo-se o histórico nas análises subsequentes. Em ambos os casos, deve armazenar a identificação do usuário, data e hora do registro.

3.25. Deve possuir capacidade para produzir alertas para cada tipo de vulnerabilidade única que for identificada. Tais alertas devem conter as seguintes informações:

3.25.1. Trecho do código vulnerável;

3.25.2. Descrição da vulnerabilidade;

3.25.3. Código de referência de bases de vulnerabilidades conhecidas, tais como CVE, VulnDB, CWE, NVD, se houver;

3.25.4. Nível de severidade;

3.25.5. Guia de remediação;

3.25.6. Exemplos de código de remediação;

3.26. Deve permitir a organização das vulnerabilidades identificadas em grupos para facilitar o processo de triagem e correção.

3.27. Deve possibilitar ao usuário a definição de filtros para os resultados de uma varredura, permitindo focar em determinados tipos de apontamento, tais como: tipo de vulnerabilidade, base de vulnerabilidade, risco potencial, API, arquivo ou diretório onde se encontra o código fonte vulnerável.

3.28. Deve permitir ao usuário desabilitar regras de análise, alterar o seu nível de severidade e identificar quais regras de detecção de vulnerabilidades foram desabilitadas.

3.29. Deve permitir que o usuário crie regras de detecção, identificando uma vulnerabilidade que a ferramenta não foi capaz de detectar nativamente.

3.30. Deve exibir de forma gráfica as informações para a identificação da vulnerabilidade, incluindo o ponto de entrada na aplicação, as saídas, bem como quaisquer outros pontos intermediários.

3.31. Deve permitir a determinação de ponto de barreira (threshold), ou seja, conjunto de precondições estabelecidas pelo administrador da ferramenta, a ser considerado no processo de construção (build) da aplicação, como condição de sucesso ou falha.

3.32. Deve permitir a comparação entre duas varreduras executadas sobre o mesmo código-fonte, apresentando as diferenças através de relatório.

3.33. Deve gerar relatórios sobre as vulnerabilidades encontradas de pelo menos duas formas: relatório gerencial e relatório detalhado com todas as informações técnicas necessárias.

3.34. Deve incluir no relatório o trecho do código fonte onde foi encontrada a vulnerabilidade.

3.35. Deve apresentar o resultado da análise em Português ou Inglês.

3.36. Deve gerar relatórios em formatos distintos, incluindo ao menos os formatos:

3.36.1. Para leitura por usuários: PDF ou HTML

3.36.2. Para processamento por outros softwares, XML, JSON ou CSV.

3.37. Deve possuir Dashboards das análises realizadas que possibilitem ao administrador configurar, dentre as informações gerenciadas pela ferramenta, aquelas que deseja apresentar em sua interface.

3.38. Deve verificar bibliotecas públicas contidas no software avaliando questões de licença de uso e vulnerabilidades

3.38.1 Deve informar qual a vulnerabilidade encontrada e qual a biblioteca afetada.

3.38.2. Deve verificar se há versão da biblioteca afetada que já tenha corrigido a vulnerabilidade.

3.38.3. Deve exibir histórico de versões de uma biblioteca informando quais versões contém vulnerabilidades e o quão confiável é a biblioteca.

C) Quanto aos serviços do fabricante associados às licenças de software

3.39. Direito de atualização de versões da solução, incluindo todos os seus componentes licenciados, durante o período de validade das licenças;

3.40. Suporte técnico remoto, em português, acionável por interface web ou por telefone, sem custo para o TRE-ES, para o esclarecimento de dúvidas quanto à utilização da solução, ou para a submissão de problemas de funcionamento da solução;

3.41. Acesso à base de conhecimento do fabricante, tanto referente ao funcionamento da solução quanto referente às vulnerabilidades de código por ela reconhecidas.

3.42 Serviço de instalação e configuração da solução

3.42.1. Instalar a solução e todos os componentes dos quais a mesma dependa para seu funcionamento, como, por exemplo, sistema operacional, banco de dados, servidor de aplicação e outros.

3.42.1.1. A instalação dos componentes deverá observar os padrões de configuração e de segurança estabelecidos pelo Tribunal, no que não conflitar com os requisitos da solução. Eventuais conflitos devem ser documentados, incluindo as soluções de contorno aplicáveis para mitigar eventuais riscos.

3.42.1.2. Incluir e configurar o acesso dos usuários pertencentes a cada perfil de acesso definido pelo Tribunal.

3.42.1.3. Configurar as integrações com ao menos uma instância dos ambientes de IDE, Versionador de códigos, Integração contínua e Qualidade de software.

3.42.1.4. Fornecer ao Tribunal, em conjunto com a entrega do documento indicativo de finalização do serviço de instalação e configuração, a documentação referente a cada uma das atividades acima descritas, de forma a possibilitar a execução de tais configurações pela equipe interna.

3.42.1.5. Opcionalmente, o serviço poderá ser realizado por meio de recursos de video-conferência e acesso remoto, por comum acordo entre o Contratante e a Contratada.

D) Repasse de conhecimento

3.43. Ministrar repasse de conhecimento sobre a solução, na forma indicada a seguir:

3.43. 1 (uma) turma para 15 (quinze) profissionais, contemplando os administradores da solução, a respeito da administração da solução, bem como das peculiaridades de instalação e configuração no ambiente do Tribunal e contemplando aspectos de desenvolvimento de software;

3.43.2. A carga horária mínima total deverá ser de 20 horas, observado o limite máximo de 4 horas diárias, compreendidas no período de 14h às 19h, em dias úteis.

3.43.3. O efetivo horário de realização do repasse para a turma poderá ser ajustado em comum acordo pelo Tribunal e pela contratada, observando-se os limites acima indicados.

3.43.4. Deverá ser ministrado por meio de recursos de video-conferência e acesso remoto.

3.43.6. Os demais recursos referentes ao repasse de conhecimento serão de responsabilidade da contratada, incluindo, mas não se limitando a, recursos humanos, licenças e instalação dos softwares necessários.

3.43.7. Deverá deverá ser baseado em documentação técnica oficial da solução de análise de vulnerabilidades e análise de bibliotecas públicas, podendo conter os devidos ajustes, desde que homologados pela representante da FABRICANTE no BRASIL e aceitos pelo Tribunal.

3.43.8. Deverá ser fornecido todo material didático, em Português do Brasil, necessário ao pleno acompanhamento dos assuntos a serem ministrados durante o referido repasse de conhecimento;

3.43.9. Deverá contemplar, no mínimo, os seguintes tópicos:

3.43.9.1. Características de instalação e configuração da solução no ambiente computacional do TRE-ES;

3.43.9.2. Administração da solução;

3.43.9.3. Conexão com o Jenkins (ambiente de integração contínua);

3.43.9.4. Conexão com o GitLab (sistema de controle de versão);

3.43.9.5. Inclusão e exclusão de projetos de software na solução;

3.43.9.6. Realização de análises de vulnerabilidades a partir da interface da própria ferramenta, bem como envolvendo as integrações com as ferramentas Jenkins, GitLab;

3.43.9.7. Realização de ciclo completo de verificação de erros/vulnerabilidades, para verificar o reflexo das correções inseridas no código e os respectivos relatórios gerados;

3.43.9.8. Identificação, classificação e gerenciamento das partes dos códigos-fontes apontados como pontos de vulnerabilidades;

3.43.9.9. Identificação, classificação e gerenciamento das bibliotecas públicas apontadas como pontos de vulnerabilidades;

3.43.9.10. Criação de novas regras e gerência das regras existentes;

3.43.9.11. Geração de relatórios;

3.43.9.12. Configuração de dashboards;

3.43.9.13. O repasse de conhecimento deverá contemplar a apresentação teórica das funcionalidades da solução e atividades práticas.

3.44. Prestar operação assistida durante 10 (dez) dias úteis após a conclusão do treinamento.

3.44.1. A operação assistida será realizada por meio de recursos de videoconferência e acesso remoto, por um profissional certificado ou acreditado pelo fabricante da solução fornecida, durante o período das 14h às 19h.

3.44.2. Este profissional será responsável por atender prontamente a qualquer solicitação de esclarecimentos por parte da equipe de administração da solução no Tribunal, ou por parte das equipes de desenvolvimento que estiverem utilizando o produto, bem como a qualquer ocorrência de problema no funcionamento da solução, incluindo suas integrações que tenham sido configuradas com os demais ambientes de desenvolvimento de software do Tribunal.

E. QUALIFICAÇÃO TÉCNICA E FINANCEIRA.

Apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove ter a licitante executado, satisfatoriamente, o fornecimento de licenças da ferramenta contratada para análise de código e bibliotecas públicas na modalidade "on premise".

Apresentar, para fins de qualificação econômico-financeira, certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante, que se encontre dentro do prazo de validade. Caso não haja prazo de validade especificado no documento, será considerado o prazo máximo de 30 (trinta) dias, contados da data de sua expedição;

F. VIGÊNCIA E DOS PRAZOS

O contrato terá validade de 36 meses.

G. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

Em termos gerais, busca-se adquirir licenças permanentes de solução de análise de código, no entanto, há que se considerar outros aspectos relacionados aos requisitos de negócio estabelecidos, que não implicam em uma dependência tecnológica propriamente dita, mas indicam a necessidade de alguns cuidados no que tange à gestão no término do contrato, como é o caso do suporte técnico e a obtenção das atualizações da ferramenta após o término do contrato.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

a) Solução similar que possa ser disponibilizada por outro órgão ou entidade da Administração Pública;

Não há solução deste tipo que atenda aos requisitos funcionais e técnicos.

b) Solução similar existente no “Portal do Software Público Brasileiro”
- http://www.softwarepublico.gov.br – (aplicável somente para o caso de Solução de Tecnologia da Informação e Comunicação que envolva software)

Não há solução deste tipo que atenda aos requisitos funcionais e técnicos.

c) Software livre ou software público.

Não há solução deste tipo que atenda aos requisitos funcionais e técnicos.

d) Solução de mercado, comercial.

Com base nos requisitos funcionais, buscou-se no mercado soluções de análise de código que fossem aderentes às necessidades. Assim, buscou-se empresas/soluções que:

1) Oferecessem análise estática de código e de bibliotecas públicas em uma única solução ou no formato de módulos de um mesmo fabricante.

2) Permitissem integração com as ferramentas já utilizadas atualmente pela equipe de desenvolvimento de software da CSGIT.

3) Licenças “on premise”, ou seja, instaladas na infraestrutura do TRE-ES.

Foram encontradas ferramentas que atendem aos requisitos especificados, tais como: Micro-focus Fortify, Synopsys, Checkmarx e HCL Software.

5. INDICAÇÃO DA STIC ESCOLHIDA

Solução de mercado, comercial.

Contratação de licenças permanentes de solução de análise estática de código e análise de bibliotecas públicas.

DESCRIÇÃO DA SOLUÇÃO

Aquisição de licença de uso de software que deverá ser instalada na modalidade “on premise” para a realização da análise estática de código fonte de aplicações e análise das bibliotecas públicas utilizadas de forma a aumentar a segurança dos softwares utilizados pelo TRE-ES.

JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

Conforme item 1.2 deste estudo.

ESTIMATIVA DE CUSTO

Valor total estimado: R$ 1.663.895,19.

ADERÊNCIA AOS REQUISITOS

Os requisitos tecnológicos que irão compor o Termo de Referência estão plenamente alinhados às necessidades da área demandante expressas através dos requisitos de negócio.

RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

A demanda prevista é aumentar a segurança das aplicações desenvolvidas pela CSGIT e aplicações de terceiros utilizadas pelo TRE-ES, a STIC escolhida irá realizar a análise do código fonte e análise das bibliotecas públicas de todas as aplicações que forem inseridas na infraestrutura do TRE-ES, de forma a auxiliar na eliminação de vulnerabilidades, aumentando a confiabilidade e segurança das aplicações

A duração do contrato deverá ser de 36 meses, porque o mercado trabalha com licenciamento por 12 ou 36 meses, por tratar-se de solução para manutenção da segurança das aplicações do TRE-ES que deverá gerar novas contratações futuras, o período de 36 meses é o mais indicado.

6. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Será necessária a criação de máquinas virtuais dentro da infraestrutura do TRE-ES para a instalação da solução.

ANÁLISE DE RISCOS

[Obrigatório para as contratações ou prorrogações, cuja estimativa de preços seja igual ou superior ao valor disposto no art. 23, inciso II, alínea "a", da Lei nº 8.666/93]

7. IDENTIFICAÇÃO DOS RISCOS

FASE DE CONTRATAÇÃO

1 - ATRASO NO TRÂMITE PROCESSUAL

FASE DE EXECUÇÃO

2 - INEXECUÇÃO CONTRATUAL

IDENTIFICAÇÃO DOS RISCOS DE DEPENDÊNCIA TECNOLOGICA

Os riscos de dependência tecnológica e o tratamento compõem o item 3.F. deste Estudo.

8. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

ANÁLISE DOS RISCOS

8.1. Probabilidade e impacto, ações de prevenção/contingência, responsáveis. Incluídos nas tabelas abaixo.

FASE DE CONTRATAÇÃO			
EVENTO 1 - ATRASO NO TRÂMITE PROCESSUAL			
Causa	Efeito	Probabilidade	Impacto
Inadequação dos aspectos técnicos do TR ao mercado, Inadequação dos aspectos administrativos do TR à expectativa da administração	Não encontrar solução para realizar a análise de código	Baixo	Médio

Plano de Resposta - Ações	Responsável
1 - Consultar empresas do ramo sobre adequação das especificações técnicas às características das soluções fornecidas pelo mercado.	Integrante Técnico
2 - Verificar/adequar/sugerir questões sobre os aspectos administrativos da contratação	Integrante administrativo

FASE DE EXECUÇÃO
EVENTO 2 - INEXECUÇÃO CONTRATUAL

Causa	Efeito	Probabilidade	Impacto
Suspensão do suporte técnico durante a execução do contrato	Impossibilidade de realização de atualizações de segurança Impossibilidade de reversão de indisponibilidade da solução por problema técnico	Baixo	Médio

Plano de Resposta - Ações	Responsável
1 - Inserir no termo de referência a necessidade disponibilidade do suporte técnico	Integrante Técnico

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

[Obrigatório para as contratações ou prorrogações, cuja estimativa de preços seja igual ou superior ao valor disposto no art. 23, inciso II, alínea "a", da Lei nº 8.666/93].

9. RECURSOS MATERIAIS E HUMANOS

Haverá necessidade de gestão da solução de conscientização para monitorar as vulnerabilidades encontradas pela solução, assim como, a realização de ações dos desenvolvedores para aplicar as soluções apontadas pela solução.

10. DESCONTINUIDADE DO FORNECIMENTO

Conforme Item 3.F deste estudo, será necessária a contratação da manutenção das atualizações da ferramenta após o término do contrato.

ANEXO A

Contratações Públicas Similares

TSE: Pregão 00058/2021 - Ata de registro de preços referente à contratação de solução de análise de código.

Petrobrás: Contratos 4600626026, 4600656121 e 4600664039

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria DG nº 154 (0740548))

Integrantes Demandantes OLGA BAYERL VITA (substituto: OTÁVIO LUBE DOS SANTOS)

Integrantes Técnicos pela área de Tecnologia da Informação LEONARDO BONN NOGUEIRA BASTOS (substituto: OLGA BAYERL VITA)

Integrante Administrativo MARCOS VENTUROTT FERREIRA (substituto: JOSE ADRIANI BRUNELLI DESTEFFANI)

Vitória, 21 de março de 2023.

Documento assinado eletronicamente por **LEONARDO BONN NOGUEIRA BASTOS**, **Integrante Técnico**, em 21/03/2023, às 17:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCOS VENTUROTT FERREIRA**, **Integrante Administrativo**, em 21/03/2023, às 17:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OLGA BAYERL VITA**, **Assistente do Núcleo de Segurança Cibernética**, em 21/03/2023, às 17:24, conforme art. 1º, III, "b", da Lei 11.419/2006.