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

TERMO DE REFERÊNCIA (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

QUADRO INFORMATIVO

OBJETO:	Solução *on premise* de software de análise estática de código e de bibliotecas públicas.
CATMAT/CATSER:	27472
QUANTITATIVOS:	1
CARACTERÍSTICAS:	Conforme item 1.3 deste TR.
DETALHAMENTO	Solução *on premise* de análise estática de código e de bibliotecas públicas para permitir scan em 65 projetos de software e atendendo a 15 desenvolvedores, contendo: - Console central de gerenciamento com dashboards - Serviço de instalação e configuração da solução, - Repasse de conhecimento para 15 pessoas - Operação assistida por 10 dias.
SUPORTE E ATUALIZAÇÃO DE SOFTWARE	36 meses

1. CARACTERIZAÇÃO DO OBJETO

1.1. DEFINIÇÃO DO OBJETO

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

1.2. DETALHAMENTO DO OBJETO

Solução *on premise* de análise estática de código e de bibliotecas públicas para permitir scan em 65 projetos de software e atendendo a 15 desenvolvedores, incluindo:

- Console central de gerenciamento com dashboards

- Serviço de instalação e configuração da solução,

- Repasse de conhecimento para 15 pessoas

- Operação assistida por 10 dias.

- Suporte suporte e atualizações por 36 meses,

1.3. ESPECIFICAÇÃO TÉCNICA MÍNIMA

A) Quanto às licenças da solução

1.3.1. 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.

1.3.2. 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

1.3.3. 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.

1.3.3.1. 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.

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

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

1.3.5.1. Common Weakness Enumeration (CWE);

1.3.5.2. Common Vulnerabilities and Exposures (CVE);

1.3.5.3. OWASP Top 10.

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

1.3.7. 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), ou container docker.

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

1.3.8.1. Oracle Linux 8 ou superior;

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

1.3.8.3. 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.

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

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

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

1.3.10. 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.

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

1.3.12. 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.

1.3.13. 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.

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

1.3.14.1. 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);

1.3.14.2. 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;

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

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

1.3.15. 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.

1.3.16. 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

1.3.17. 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:

1.3.17.1. Java 11 com retrocompatibilidade até Java 6;

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

1.3.17.3. Javascript, Typescript;

1.3.17.4. PHP versões: 5, 7 e superiores;

1.3.17.5. XML;

1.3.17.6. HTML;

1.3.17.7. PL/SQL

1.3.17.8. Python;

1.3.17.9. Mobile (Android e IOS);

1.3.17.10. C#

1.3.17.11. Asp.net

1.3.17.12. Docker (dockerfile)

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

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

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

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

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

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

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

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

1.3.19. As análises de vulnerabilidades devem poder ser realizadas por submissão direta na plataforma e por meio da solução de integração contínua especificados no item 1.3.14.1.

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.

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

1.3.22. 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.

1.3.23. 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.

1.3.24. 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.

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

1.3.25.1. Trecho do código vulnerável;

1.3.25.2. Descrição da vulnerabilidade;

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

1.3.25.4. Nível de severidade;

1.3.25.5. Guia de remediação;

1.3.25.6. Exemplos de código de remediação;

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

1.3.27. 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.

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

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

1.3.30. 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.

1.3.31. 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.

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

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

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

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

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

1.3.36.1. Para leitura por usuários: PDF ou HTML

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

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

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

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

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

1.3.38.3. 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

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

1.3.40. 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;

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

1.3.42 Serviço de instalação e configuração da solução

1.3.42.1. 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.

1.3.42.1.1. 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.

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

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

1.3.42.1.4. 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.

1.3.42.1.5. 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

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

1.3.43. 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;

1.3.43.2. 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.

1.3.43.3. 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.

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

1.3.43.6. 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.

1.3.43.7. 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.

1.3.43.8. 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;

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

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

1.3.43.9.2. Administração da solução;

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

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

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

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

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

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

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

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

1.3.43.9.11. Geração de relatórios;

1.3.43.9.12. Configuração de dashboards;

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

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

1.3.44.1. 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.

1.3.44.2. 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.

1.4. QUANTIFICAÇÃO OU ESTIMATIVA PRÉVIA

Quantidade: 1

1.5. ESTIMATIVA DE PREÇO

O valor estimado para a contratação é de R$ 1.663.895,19 (um milhão, seiscentos e sessenta e três mil, oitocentos e noventa e cinco reais e dezenove centavos).

1.6. DA PROPOSTA

Na proposta deverá ser indicada a formação do preço conforme tabela abaixo:

Informar a Marca/Modelo da Solução					
Item	Descrição	Unidade	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1	Solução de análise estática de código (SAST)				
2	Solução de análise de bibliotecas públicas				
3	Console de gerência				
4	Suporte e atualizações por 36 meses	Meses	36		
5	Serviço de Instalação	Serviço	1		
6	Repasse de conhecimento	Pessoas	15		
7	Operação Assistida	Dias	10		
8	Outros (especificar)				
VALOR TOTAL DA PROPOSTA		R$			

Observação: Como soluções de fabricantes diferentes possuem formas de cobrança diferentes, não definimos a unidade nem a quantidade dos itens, visando possibilitar a participação de todos, ampliando a competição. Atendidas todas as exigências e apresentando o menor preço total, esses fatores não trazem prejuízo à contratação.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. 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.

2.2. ALINHAMENTO ESTRATÉGICO

A contratação está alinhada ao PDTIC, princípios P6, P8, diretrizes D3, D6, e objetivo O7.

2.3. REFERÊNCIA AOS ESTUDOS TÉCNICOS PRELIMINARES

Os estudos técnicos realizados encontram-se incluídos no documento nº 0926250

2.4. RELAÇÃO ENTRE A DEMANDA PREVISTA E A STIC A SER CONTRATADA

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.

Atualmente a CSGIT possui 65 sistemas ativos, o que justifica a quantidade de projetos que precisam ser analisados pela solução selecionada. Será necessário treinamento e acompanhamento inicial para melhor aproveitamento da solução, há 14 desenvolvedores atualmente na CSGIT e 1 assistente do núcleo de segurança cibernetica que deverão participar do treinamento para utilização da solução.

2.5. JUSTIFICATIVA DA STIC ESCOLHIDA

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.

As soluções encontradas aceitam as linguagens de programação utilizadas pela CSGIT, permitem a integração com as ferramentas já utilizadas com a unidade, possibilitam a identificação de trechos de código e bibliotecas de terceiros contendo vulnerabilidades e são capazes de indicar soluções para as vulnerabilidades encontradas. Dessa forma, atendem de forma satisfatória aos requisitos deste Termo de Referência.

3. ESTRATÉGIA DA CONTRATAÇÃO

3.1. FORMA DE PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

O objeto da licitação será adjudicado ao licitante que ofertar o MENOR PREÇO GLOBAL. Não haverá parcelamento do objeto.

3.2. MODALIDADE E TIPO DE LICITAÇÃO

A modalidade de licitação é o **Pregão Eletrônico**, considerando a obrigatoriedade contida no §1º, artigo 1º, do Decreto n°10.024/2019.

Em cumprimento ao Art. 28, inciso II, da Resolução TRE/ES n° 261/2018, o tipo de licitação indicada para a contratação em tela é o de **menor preço global** e para a habilitação, o licitante deverá:

1 – estar inscrito no SICAF, com a documentação obrigatória regularizada;

2 – apresentar prova de regularidade com a **Fazenda Municipal** da sede ou do domicílio da empresa licitante;

3 – apresentar prova de regularidade com a Justiça do Trabalho;

4 – preencher, no momento do envio da proposta comercial, no sistema Comprasnet, a seguinte declaração:

a) De que cumpre o disposto no inciso XXXIII do art. 7° da Constituição da República Federativa do Brasil de 1988, conforme prescreve o inciso V do art. 27 da Lei n°. 8.666/1993.

5 – apresentar qualificação técnica;

6 – apresentar qualificação econômico-financeira.

3.3. MARGEM DE PREFERÊNCIA

Há previsão de aplicação de margens de preferência conforme disposto no Decreto nº 7.174/2010.

3.4. CLASSIFICAÇÃO ORÇAMENTÁRIA

SITUAÇÃO	Há disponibilidade orçamentária
PROGRAMA DE TRABALHO	02122003321EE0001 - Gestão da Política de Segurança da Informação e Cibernética na Justiça Eleitoral
PLANO ORÇAMENTÁRIO	SEG0 - Segurança da Informação
NATUREZA DA DESPESA	449040 – Serviços de Tecnologia da Informação e Comunicação - PJ
SUBITEM DA DESPESA	05 – Aquisição de software pronto
PLANO INTERNO	SIN SOFTWR
VALOR CONSIDERADO	R$ 1.663.895,19 (Conforme despacho Secom 0829751)

3.5. VIGÊNCIA DA CONTRATAÇÃO

Etapa	Descrição	Prazo
1	**Assinatura do Contrato**	**Dia D**
2	Disponibilização da infraestrutura para instalação da solução Convocar reunião inicial com a CONTRATADA	D+5
2	**Entrega da fase 1 - Liberação das licenças e instalação da plataforma na infraestrutura do TRE-ES**	**D+15 (E1)**
3	Apresentação do documento fiscal - Fase 1	E1+2
4	Aceite Técnico Definitivo - Fase 1	E1+4

5	**Pagamento - Fase 1 (80% do total)**	E1+14
6	Passagem de conhecimento	E1+15
7	Operação Assistida	E1+25
8	**Entrega da fase 2 - Passagem de Conhecimento e Operação Assistida**	E1+25
9	Apresentação do documento fiscal - Fase 2	E1+27
10	Aceite Técnico Definitivo - Fase 2	E1+27
11	**Pagamento - Fase 2 (20% do total)**	E1+37
12	**Vigência das Licenças de Uso**	**E1+36 meses**

Tab. 1 - Cronograma executivo

*** Todos os prazos em dias úteis. Havendo antecipação das entregas, os prazos posteriores são automaticamente antecipados.**

3.6. QUALIFICAÇÃO TÉCNICA E ECONÔMICO-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 pelo menos uma licença da solução proposta 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;

3.7. DO ENVIO DA AMOSTRA

3.7.1. O licitante melhor classificado na etapa de lances, deverá enviar uma amostra para a equipe técnica do TRE-ES que deverá realizar testes para verificação do atendimento de todos os requisitos especificados no item 1.3 e seus subitens, deste Termo de Referência.

3.7.2. A proponente deverá especificar à equipe técnica do TRE-ES os requisitos da máquina que deverá ser disponibilizada na infraestrutura do TRE-ES para a instalação da solução ofertada, também poderá ser aceita a disponibilização da amostra por meio de um container docker. Devendo também fornecer um telefone e e-mail da pessoa que irá auxiliar nas configurações.

3.7.2.1 Caso seja necessária a máquina virtual, a proponente terá 1 dia para informar as configurações mínimas necessárias e a equipe técnica do TRE-ES terá o prazo de 2 dias úteis para a criação da máquina virtual conforme especificações.

3.7.3. A proponente deverá, no prazo de até 5 dias úteis, disponibilizar uma licença da solução contendo todas as funcionalidades necessárias para o atendimento de todos os requisitos técnicos contidos neste TR, que deverá ser instalada na infraestrutura do TRE-ES.

3.7.3.1. O proponente deverá auxiliar a equipe técnica do TRE-ES a instalar da solução na infraestrutura do TRE-ES.

3.7.5. A equipe técnica do TRE-ES terá o prazo de 5 dias úteis, a partir da disponibilização da amostra, para a realização dos testes necessários para a verificação da solução disponibilizada.

3.7.5.1. A proponente deverá estar disponível para resolver quaisquer dúvidas quanto às configurações ou uso da solução durante o período de testes.

3.7.6. Após a realização dos testes a equipe técnica deverá emitir um parecer quanto a aceitação ou não da solução.

3.7.6.1. Caso a solução não seja aceita, deverá constar no parecer quais itens não foram atendidos pela solução.

3.7.6.2. Qualquer item especificado neste Termo de Referência não atendido pela solução da proponente ensejará a desclassificação da proponente.

4. DEFINIÇÃO DAS RESPONSABILIDADES DO CONTRATANTE

4.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

4.2. Acompanhar, fiscalizar e atestar a execução contratual, bem como indicar as ocorrências verificadas.

4.3. Designar servidor ou comissão de servidores para fiscalizar a execução do objeto contratual.

4.4. Convocar reunião inicial com a Contratada para apresentação do preposto, entrega dos Termos de Sigilo e Confidencialidade e outros documentos relevantes, e esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

4.5. Permitir que os funcionários da contratada, desde que devidamente identificados, tenham acesso aos locais de entrega.

4.6. Recusar qualquer material entregue em desacordo com as especificações constantes do Termo de Referência ou com defeito.

4.7. Efetuar o pagamento à contratada segundo as condições estabelecidas neste Termo de Referência.

5. DEFINIÇÃO DAS RESPONSABILIDADES DA CONTRATADA

5.1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste Termo de Referência.

5.2. Responsabilizar-se pelas despesas decorrentes da execução dos serviços objeto deste Termo de Referência.

5.3. Informar nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TRE-ES, bem como manter os dados atualizados durante toda a fase de execução da

contratação.

5.3.1. Toda a comunicação referente à execução do objeto será realizada através do e-mail informado pela Contratada no momento da assinatura do contrato.

5.3.2. A comunicação será considerada recebida após a confirmação de entrega automática encaminhada pelo Outlook, independentemente de confirmação de recebimento por parte da contratada, ficando sob sua responsabilidade a verificação da conta de e-mail.

5.3.3. A comunicação só será realizada de forma diversa quando a legislação exigir ou quando a contratada demonstrar ao fiscal os motivos que justifiquem a utilização de outra forma.

5.4. Participar de reunião inicial após a formalização contratual, a ser convocada pelo Contratante.

5.5. Acatar as recomendações efetuadas pelo fiscal do contrato.

5.6. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do Termo de Referência.

5.7. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do TRE-ES, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).

5.8. Comunicar ao TRE-ES, por escrito, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais

5.9. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TRE-ES, não os divulgando, copiando, fornecendo ou mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à contratada, durante e após a vigência do contrato.

5.9.1. Tal exigência se dará de acordo com o “Termo de Sigilo e Confidencialidade” cujo modelo consta do Adendo I deste Termo de Referência, a ser assinado pelos profissionais da contratada que executarão os serviços definidos neste Termo de Referência.

5.10. Manter, durante a execução do contrato, as condições de habilitação exigidas na licitação.

5.10.1. Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a contratada terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.

5.11. Responsabilizar-se pelos encargos fiscais e comerciais resultantes da contratação.

5.11.1. A inadimplência da contratada com referência aos encargos suportados não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto do contrato.

5.12. Ceder ao Tribunal os direitos de propriedade intelectual e direitos autorais sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, contemplando a documentação gerada, procedimentos estabelecidos para a utilização da solução e quaisquer outros documentos que tenham sido elaborados.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. FIXAÇÃO DAS ROTINAS DE EXECUÇÃO DO CONTRATO

6.2 ASSINATURA DO CONTRATO

Devem constar as seguintes informações no instrumento contratual, para fins da adequada condução das rotinas de execução contratual:

- Nome completo, telefone e email do contato indicado pela CONTRATADA.
- Os canais de comunicação formais que a CONTRATANTE deverá usar para acionar a operação assistida.
- Os canais de comunicação formais que a CONTRATANTE deverá usar para acionar o suporte técnico relativo a problemas na plataforma.
- O(s) endereço(s) eletrônico(s) da CONTRATANTE (Justiça Eleitoral) que servirá (ão) como canal de comunicação formal da CONTRATADA com a CONTRATANTE.
- Termo de sigilo e confidencialidade adendo ao contrato principal.

RECEBIMENTO, INSTALAÇÃO E ACEITE DAS LICENÇAS

6.3. A documentação que comprova a aquisição das licenças deve ser encaminhada por meio digital para o e-mail da CONTRATANTE indicado no contrato, no prazo estabelecido neste termo de referência.

6.4 A CONTRATANTE tem prazo de 5 dias úteis para disponibilizar infraestrutura para a CONTRATADA.

6.5. A instalação deverá ser efetuada na infraestrutura da CONTRATANTE pela CONTRATADA.

6.6 Um e-mail formal da contratada informando o término da instalação e a entrega da documentação prevista no **subitem 1.3.42.1.4,** caracterizam a entrega E1 e o RECEBIMENTO PROVISÓRIO.

6.7. O integrante técnico deverá certificar-se de que o(s) colaborador(es) da CONTRATADA assinem o **TERMO DE CIÊNCIA E ACEITE DAS CONDIÇÕES DE MANUTENÇÃO DE SIGILO (ADENDO I)** antes de conceder acesso à infraestrutura do TRE-ES.

6.8. O fiscal técnico do contrato deverá acompanhar a instalação da solução na infraestrutura do TRE-ES.

6.9 O fiscal técnico do contrato verificará a autenticidade das licenças na plataforma no prazo de até 4 (quatro) dias úteis após a instalação.

6.10. O recebimento da nota fiscal e a verificação da autenticidade das licenças na plataforma, caracterizará o RECEBIMENTO DEFINITIVO, relativo à entrega das licenças, ensejando o pagamento de 80% do valor total da solução.

RECEBIMENTO E ACEITE DO REPASSE DE CONHECIMENTO E OPERAÇÃO ASSISTIDA

6.11.Deverá ser agendada com a equipe técnica da CONTRATANTE a passagem de conhecimento para os desenvolvedores, administradores e gestores.

6.12. A operação assistida só poderá ser iniciada após o término do treinamento.

6.13. O integrante técnico deverá certificar-se de que o(s) colaborador(es) da CONTRATADA assinem o **TERMO DE CIÊNCIA E ACEITE DAS CONDIÇÕES DE MANUTENÇÃO DE SIGILO (ADENDO I)** antes de iniciar a operação assistida.

6.14. Conforme subitem 3.5, o prazo máximo para finalização do repasse de conhecimento é de 30 dias úteis após assinatura do contrato e o prazo máximo para término da operação assistida é de 40 dias úteis após a assinatura do contrato.

6.15. Finalizado o período de operação assistida, o fiscal técnico emitirá, no prazo de até 2 (dois) dias úteis, o RECEBIMENTO DEFINITIVO dos serviços, verificando se foram cumpridas todas as exigências previstas no subitem 1.3.43 deste Termo de Referência, ensejando o pagamento de 20% do valor total da solução.

PROCEDIMENTOS DE ROTINA

6.16. O gestor contratual, com apoio da equipe de gestão, registrará eventuais ocorrências relativas ao contrato e comunicará à Administração sempre que houver situações que possam implicar em sanções à CONTRATADA.

6.17. A CONTRATADA deverá comunicar formalmente à CONTRATANTE, com pelo menos 10 dias de antecedência, sobre eventual alteração nos canais de comunicação com a empresa.

6.18. A CONTRATADA deverá informar a CONTRATANTE, através do endereço eletrônico estabelecido no contrato, os canais de comunicação formais para abertura de chamados técnicos relativos a problemas na plataforma.

6.19. Durante a execução do contrato, havendo necessidade de acesso da CONTRATADA à infraestrutura da CONTRATANTE, o integrante técnico deverá certificar-se de que o(s) colaborador(es) da CONTRATADA assine(m) o **TERMO DE CIÊNCIA E ACEITE DAS CONDIÇÕES DE MANUTENÇÃO DE SIGILO (ADENDO I)** antes de iniciar o acesso.

6.20. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

É vedada às partes a utilização de todo e qualquer dado pessoal, repassado em decorrência da execução contratual, para finalidade distinta da contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

Para fins de execução do objeto contratado e de cumprimento de obrigação legal ou regulatória, o Contratante poderá proceder ao tratamento dos dados pessoais dos representantes legais da Contratada, inclusive para publicação nos portais de Transparência do Contratante;

6.21. FORMA DE PAGAMENTO

6.21.1. Será realizado pagamento em duas parcelas, sendo **80% do total pago após a instalação e validação das licenças adquiridas** e **20% após o repasse de conhecimento e operação assistida**.

6.21.2. A nota fiscal/fatura deverá ser apresentada pela Contratada ao Gestor contratual;

6.21.3. O pagamento fica condicionado à prova de regularidade perante a Fazenda Nacional, a Previdência Social e junto ao FGTS;

6.21.4. O prazo de pagamento é de **até 10 (dez) dias úteis** após o aceite definitivo, conforme estabelecido no **item 3.5** deste Termo de Referência.

6.22. MODELOS DE TERMOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO

6.22.1 Deve ser assinado termo de sigilo e confidencialidade (ADENDO I) 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 deste serviço.

6.22.2 Os funcionários da CONTRATADA que, a qualquer tempo do contrato, precisarem ter acesso às informações da CONTRATANTE deverão assinar o **TERMO DE CIÊNCIA E ACEITE DAS CONDIÇÕES DE MANUTENÇÃO DE SIGILO (ADENDO I)** antes de atuarem nas atividades. Caberá ao fiscal técnico e ao gestor contratual, antes de conceder o acesso às informações da CONTRATANTE, providenciar junto a CONTRATADA a assinatura do referido termo pelos profissionais envolvidos das atividades.

7. MODELO DE GESTÃO DO CONTRATO

7.1. FIXAÇÃO DOS CRITÉRIOS DE ACEITAÇÃO

Conforme **subitens 6.3 a 6.15** deste Termo de Referência.

7.2. INDICAÇÃO DOS PROCEDIMENTOS MÍNIMOS DE TESTE E INSPEÇÃO

Conforme **subitens 6.3 a 6.15** deste Termo de Referência.

7.3. RETENÇÕES OU GLOSAS

Não se aplica à presente contratação.

7.4. SANÇÕES ADMINISTRATIVAS

7.1. Atraso na Entrega do Objeto.

Item	Descumprimento	Percentual diário	Limite de dias	Percentual total	Base de incidência
1	Atraso na entrega das Licenças	0,5%	20	10%	Valor do Contrato
2	Prazo excepcional para entrega das Licenças	0,5%	20	10%	Valor do Contrato
3	Atraso no início do treinamento ou operação assistida	0,5%	20	10%	Valor do Objeto em Atraso
4	Prazo excepcional para entrega do treinamento ou operação assistida	0,5%	20	10%	Valor do Objeto em Atraso

5	Inexecução Contratual	-----	-----	30%	Valor do Contrato

* Os prazos previstos nos itens 1 e 3 são automáticos, sem necessidade de autorização da Administração, porém com aplicação das sanções previstas.
* Os prazos excepcionais previstos nos itens 2 e 4 precisam ser autorizados pela Administração, após avaliação da justificativa da empresa e oitiva dos setores técnicos.
* A extrapolação dos prazos previstos em 1 e 3, caso não haja autorização de prazos excepcionais, caracterização a Inexecução Contratual.
* A extrapolação dos prazos extraordinários previstos em 2 e 4, caso concedidos, caracterizarão a Inexecução Contratual.

7.2. Outras Sanções com Grau de Severidade

7.2.1. Grau de Severidade Leve

L1 – Notificação de Descumprimento Contratual – Quando for o caso, a CONTRATADA será notificada e deve adequar-se à exigência contratual formalizada pela Equipe de Gestão Contratual em até 10 (dez) dias úteis, contados a partir da data de recebimento da notificação. Findo o prazo e mantendo-se os motivos que levaram a notificação, a CONTRATADA estará sujeita a multa diária de 2 (duas) vezes o valor unitário da licença contratada, limitados ao total de até 30 (trinta) dias corridos, quando restará configurada uma inexecução contratual.

7.2.2. Grau de Severidade Moderado

M1 – Multa fixa (MLT-FIXA) de 5 (cinco) vezes o valor unitário da licença de usuário contratada OU multa diária (MLT-DIÁRIA) de 50% do valor unitário da licença de usuário contratada. Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 10 (dez) dias corridos, quando restará configurada uma inexecução contratual.

M2 – Multa fixa (MLT-FIXA) de 25 (vinte e cinco) vezes o valor unitário da licença de usuário contratada OU multa diária (MLT-DIÁRIA) de 5 (cinco) vezes o valor unitário da licença de usuário contratada. Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 5 (dias) dias corridos, quando restará configurada uma inexecução contratual.

M3 – Multa fixa (MLT-FIXA) de 50 (cinquenta) vezes o valor unitário da licença de usuário contratada OU multa diária (MLT-DIÁRIA) de 10 (dez) vezes o valor unitário da licença de usuário contratada. Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 5 (cinco) dias corridos, quando restará configurada uma inexecução contratual.

7.2.3. Grau de Severidade Grave/Inexecução Contratual

Multa de 30% (trinta por cento) sobre o objeto inexecutado e ressarcimento à contratante o valor correspondente ao período inexecutado, com as devidas atualizações.;

G1 – Rescisão contratual

G2 – Suspensão por até 5 (cinco) anos de participação em licitação;

G3 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

7.2.4. Relação de Eventos

A Relação de Eventos apresenta um conjunto não exaustivo dos eventos causadores de sanções contratuais. Para cada um dos eventos descritos, uma ou mais sanções poderão ser aplicadas. A tabela a seguir apresenta uma amostra do relacionamento de eventos e sanções. O número dentro da tabela descreve o número de vezes (primeira ocorrência e demais reincidências) que o evento ocorreu durante a vigência do contrato (nota-se que, de acordo com os critérios, a reincidência aumentará o grau de severidade).

RELAÇÃO DE EVENTOS								
Nº	Evento	Grau de Severidade						
		Leve	Moderado			Grave		
		L1	M1	M2	M3	Inexecução Contratual		
						G1	G2	G3
1	Apresentar documentação falsa.					1ª	1ª	1ª
2	Não mantiver a Proposta.					1ª	1ª	1ª
3	Fraudar a execução do contrato.					1ª	1ª	1ª
4	Comportar-se de modo inidôneo.					1ª	1ª	1ª
5	Fizer declaração falsa ou cometer fraude fiscal.					1ª	1ª	1ª
6	Negar-se a assinar o contrato no prazo estabelecido.					1ª	1ª	1ª
7	Não designar Contato para Operação Assistida	1ª						
8	Deixar de substituir Contato para Operação Assistida no prazo de 10 (dez) dias úteis após solicitação formal da contratante (MLT-DIÁRIA)	1ª	2ª	3ª	4ª	5ª		
9	Quando o Contato para Operação Assistida não apresentar-se em reunião pré-agendada (MLT-FIXA)		1ª	2ª	3ª a 6ª	7ª		

10	Impossibilidade estabelecer comunicação com o contato técnico por mais de 2 (dois) dias úteis através dos canais formais. (MLT-DIÁRIA)		1ª	2ª	3ª a 4ª	5ª		
11	Impossibilidade estabelecer comunicação com o suporte técnico por mais de 1 (um) dia útil através dos canais formais. (MLT-DIÁRIA)		1ª a 5ª	6ª a 15ª	16ª a 20ª	21ª		
12	Não honrar o prazo de vigência do suporte e manutenção das atualizações ou interromper totalmente o acesso ao suporte ou atualizações por período superior a 7 dias dentro de um mês.					1ª	1ª	1ª
13	Não responder dentro do prazo estabelecido os esclarecimentos solicitados pela fiscalização do contrato no que diz respeito ao cumprimento do objeto contratado, mesmo os de ordem técnica, operacional ou administrativa. (MLT-FIXA)	1ª	2ª	3ª	4ª a 10ª	11ª		
14	Deixar de comunicar formalmente à CONTRATANTE, com pelo menos 10 dias de antecedência, sobre a alteração dos canais formas de comunicação definidos em contrato.		1ª a 2ª	3ª a 4ª	5ª a 7ª	8ª		
15	Descumprir qualquer dispositivo do termo de sigilo, da política de segurança ou do código de ética da CONTRATANTE					1ª	1ª	1ª
16	Não guardar sigilo dos dados processados no TRE/ES e/ou divulgar sem autorização formal do Gestor ou Fiscal Técnico do Contrato, informações tratadas nas dependências da CONTRATANTE.					1ª	1ª	1ª
17	Deixar de comunicar formalmente a Equipe de Gestão Contratual as eventuais irregularidades (MLT-FIXA)		1ª	2ª	3ª	4ª		
18	Descumprimento total ou parcial das obrigações assumidas por mais de 30 (trinta) dias corridos para o caso de notificações L1, 10 (dez) dias corridos no caso de multas com grau de severidade M1 e 5 (cinco) dias corridos para multas com grau de severidade M2 e M3, cuja justificativa não for acatada pelo TRE/ES					1ª	1ª	1ª
19	Qualquer outra obrigação prevista não cumprida pela CONTRATADA, incluindo as exigidas do gerente técnico e dos demais profissionais alocados. (MLT-FIXA ou MLT-DIÁRIA), conforme o caso	1ª	2ª	3ª	4ª em diante			

MLT-DIÁRIA: Multa diária calculada em função de percentuais estabelecidos para M1, M2 e M3.

MLT-FIXA: Multa fixa indicadas em M1, M2 e M3, parcela única.

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 17:18, 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.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0926251** e o código CRC **75DDBF5C**.