TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL

ESTUDO PRELIMINAR - CONTRATAÇÕES DE TIC

ANEXO I.a

1. ESTUDO TÉCNICO PRELIMINAR - SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

1.1 SOLUÇÃO DE TI A CONTRATAR

O presente estudo preliminar visa a contratação do suporte das licenças da Ferramenta de Gestão de Vulnerabilidades atualmente implantada no TRE-MS.

1.2 EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A equipe responsável pelo planejamento da contratação é composta pelos seguintes membros:

Tipo	Nome	Lotação	E-mail
Demandante	Antônio Mendes Barata Segundo	STI/GABSTI	antonio.barata@tre-ms.jus.br
Técnico	Marcelo Silva de Novaes	STI/CITIS	marcelo.novaes@tre-ms.jus.br
Administrativo	Graziela Gonçalves Silva Jurado	SAF/CRM/SLC	graziela.goncalves@tre-ms.jus.br

1.3 DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS E DA NECESSIDADE DA CONTRATAÇÃO

1.3.1 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Manter a busca constante pela proteção do Tribunal contra invasões externas, prezando pela imagem do órgão.

1.3.2 IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

Manter a identificação das vulnerabilidades em sistemas e aplicações, bem como nos equipamentos de infraestrutura de TI (servidores, redes etc)

1.3.3 DEMAIS REQUISITOS

1. A solução deve estar licenciada e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware) para no mínimo 250 IPs;

2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

3. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

4. Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);

5. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;

6. Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;

7. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;

8. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

9. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:
    10.1. Por sistema operacional;
    10.2. Por um determinado software instalado;
    10.3. Por Ativos impactados por uma determinada vulnerabilidade.

11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);

12. Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

13. Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

14. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;

15. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;

16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
    16.1. CVSSv3 Impact Score;
    16.2. Idade da Vulnerabilidade;
    16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
    16.4. Número de produtos afetados pela vulnerabilidade;

17. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo feeds de inteligência de ameaças ao vivo;

18. Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM;

19. Deve possuir uma API para automação de processos e integração com aplicações

ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;

20. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

21. A solução deve possuir conectores para, no mínimo, as seguintes plataformas:
a) Amazon Web Service (AWS);
b) Microsoft Azure;
c) Google Clound Platform.

22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV, HTML e no formato de texto que poderá ser DOCX ou RTF;

23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
a) Execução de verificação completa do sistema (rede), adequada para qualquer host;
b) verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
c) Autenticação de hosts e enumeração de atualizações ausentes;
d) Execução de varredura simples para descobrir hosts ativos e portas abertas;
e) Utilização de um scanner para verificar aplicativos da web;
f) Avaliação de dispositivos móveis
g) Auditoria de configuração de serviços em nuvem de terceiros;
h) Auditoria de configuração dos gerenciadores de dispositivos móveis;
i) Auditoria de configuração dos dispositivos de rede;
j) Auditoria de configurações do sistema em relação a uma linha de base conhecida;
k) Detecção de desvio de segurança Intel AMT;
l) Verificação de malware nos sistemas Windows e Unix;

26. Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

27. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no minímo:
a) Bancos de dados;
b) Hypervisors (no mímino VMWare ESX/ESXi);
c) Dispositivos móveis;
d) Dispositivos de rede;
e) Endpoints;
f) Aplicações;

28. A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;

29. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.

32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

33. Configuração de segurança e acesso à gerência da solução:
a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) Os dados em transito devem usar ao menos o algoritimo TLS 1.2 de chave 2048 bits;

c) Os dados em transito devem ser criptografados ao menos com o algoritimo AES-128 bits;

d) Os algoritimos de hash devem usar ao menos o algoritimo SHA-256;

e) Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;

f) Os dados armazenados devem ser criptografados ao menos com o algoritimo AES-256 bits;

g) Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

h) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

i) A empresa contratada não deverá ter acesso a rede interna da contratante e todo trafego de dados deverá ser de saída e iniciado pelos scanners (on-premises).

34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

35. Dos Relatórios:

35.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;

35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;

35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;

35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;

35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;

35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;

37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

37.1. Hosts verificados sem credenciais;

37.2. Top 100 Vulnerabilidades mais criticas;

37.3. Top 10 Hosts infectados por Malwares;

37.4. Hosts exploráveis por Malwares;

37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

37.6. Vulnerabilidades críticas e exploráveis;

37.7. Máquinas com vulnerabilidades que podem ser exploradas;

38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;

39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 250 IPs;

41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);

42. Deve permitir a configuração de vários painéis e widgets;

43. Deve ser capaz de medir e reportar ameaças;

44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;

45. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;

46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

47. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;

48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

49. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

50. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;

51. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve ser capaz de ser reiniciado de onde parou;

52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;

53. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais.

56. A solução deve possuir módulo para realizar varreduras de vulnerabilidades para no mínimo 5 aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;

56.1. A solução de análise deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo no mínimo, mas não limitando-se a base de ameaças apontadas pelo OWASP Top 10, CWE e WASC;

56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;

56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);

56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;

56.5. Para varreduras do tipo extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

a) Cookies, Headers, Formulários e Links;
b) Nomes e valores de parâmetros da aplicação;
c) Elementos JSON e XML;
d) Elementos DOM;

56.6. Deverá também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

56.7. A solução de análise deve suportar a integração com o softwares de automação de testes para permitir sequências de autenticação complexas;

56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;

56.9. Suporte a ferramentas para construção de requisições e análise de respostas de aplicações WEB, API's e WebServices, tais como Postman Collections;

56.10. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;

56.11. Deve ser capaz de utilizar scripts customizados de crawling com parâmetros definidos pelo usuário;

56.12. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

56.13. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

56.14. Deve ser capaz de instituir no mínimo os seguintes limites:

a) Número máximo de URLs para crawling e navegação;

b) Número máximo de diretórios para varreduras;

c) Número máximo de elementos DOM;

d) Tamanho máximo de respostas;

e) Tempo máximo para a varredura;

f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;

g) Número máximo de requisições HTTP(S) por segundo;

56.15. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

56.16. Deve suportar o envio de notificações por email;

56.17. Deverá ser compatível com avaliação de web services REST e SOAP;

56.18. A solução de análise deve suportar os seguintes esquemas de autenticação:

a) Autenticação Básica (Digest);

b) NTLM;

c) Autenticação de Cookies;

56.19. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;

56.20. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

56.21. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

56.22. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;

56.23. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

56.24. Serviço de Detecção de Malware:

a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;

b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;

c) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos XML, HTML e PDF.

57. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:

a) WordPress;

b) IIS 6.x e IIS 10.x;

c) ASP 6;

d) NET 2;

e) Apache HTTPD 2.2.x e 2.4.x;

f) Tomcat 6.x, 7.x, 8.x e superiores;

g) Jetty 8 e superiores;

h) Nginx;

i) PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;
j) Java 1.5, 1.6, 1.7 e 1.8 e superiores;
k) Jboss 4.x e 7.x e superiores;
l) WildFly 8 e 10 e superiores;
m) Plone 2.5.x e 5.2.1.41.x e superiores;
n) Zope;
o) Python 2.4.4 e superiores;
p) J2EE;
q) Ansible;
r) Joomla;
s) Moodle;
t) Docker Conteiner;
u) Elk;
v) GIT;
w) Grafana; e
x) Redmine.

Requisitos de Segurança

1. A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.644/2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Mato Grosso do Sul aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

2. O Tribunal Regional Eleitoral do Mato Grosso do Sul terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

3. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

2. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS, COM JUSTIFICATIVA PARA A QUANTIDADE

Quantidade é igual à prevista no DOD?

(X) Sim

( ) Não. Justifique:

( ) Não se aplica

3. ANÁLISE DE SOLUÇÕES POSSÍVEIS

3.1 IDENTIFICAÇÃO DAS DIFERENTES SOLUÇÕES DE TIC

Id	Descrição da solução (ou cenário)
1	Solução utilizando Softwares livres
2	Solução de gerenciamento e armazenamento na nuvem (on cloud)
3	Solução de gerenciamento e armazenamento no Tribunal (on premise)

3.2 ANÁLISE COMPARATIVA DE SOLUÇÕES

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		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
A solução apresenta observância ao Modelo Nacional de Interoperabilidade?	Solução 1			X
	Solução 2			X
	Solução 3			X
A solução apresenta observância ao Modelo de Requisitos para sistemas informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	Solução 1			X
	Solução 2			X
	Solução 3			X

3.3 PESQUISA DE PREÇOS DE MERCADO

Id	Descrição da solução (ou cenário)
1	Solução utilizando Softwares livres
2	Solução de gerenciamento e armazenamento na nuvem (on cloud)
3	Solução de gerenciamento e armazenamento no Tribunal (on premise)

UASG: 806030 - SERPRO - SEDE BRASILIA - Pregão nº 255/2023 - Item 01 - R$ 64.900,00

Contrato TRE/MS nº 45/2020 - 103.928,83 (Valor de aquisição. Conforme informado informalmente pelo fornecedor, o valor de renovação gira em torno de 60% do valor de aquisição - R$ 62.357,30)

Proposta da empresa SERVIX: R$ 103.437,00 (36 meses - aproximadamente R$ 2.873,25)

Proposta da empresa SERVIX: R$ 169.165.40 (60 meses - aproximadamente R$ 2.819,42)

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução 1 - Baseada em Software Livre atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Livre é que os relatórios fornecidos pela ferramenta não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

Solução 2 - Baseada em nuvem (cloud computing) apresenta facilidade de gerenciamento, valor de aquisição adequado e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Tods os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Porém, como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis não é recomendável estarem armazenados em nuvem pública.

5. ANÁLISE E COMPARAÇÃO ENTRE OS CUSTOS TOTAIS DAS STICs

5.1 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

O TRE-MS já possui implantado a solução de Gestão de Vulnerabilidades do fabricante Tenable. Para resguardar o conhecimento sedimentado na equipe de segurança cibernética, optamos por buscar a renovação do licenciamento da mesma solução. Sendo assim, o custo total da solução foi baseado nessa ferramenta.

Item	Descrição	CATSER	Qtde	Preço 1	Preço 2	Preço 3	Valor Médio	Valor Total
01	Renovação de Subscrição Tenable (TSCCV-P e TSCCV-M) pelo período de 36 (trinta e seis) meses	15741	05	R$ 64.900,00	R$ 62.357,30	103.437,00	R$ 76.898,10	R$ 384.490,50
TOTAL								**R$ 384.490,50**

Preço 1 - O preço 1 foi obtido através de consulta ao Painel de Preços (https://paineldeprecos.planejamento.gov.br/) e é referente a contratação dos itens 1, do Pregão nº 255/2023, do SERPRO - SEDE BRASILIA - R$ 64.900,00.

Preço 2 - O preço 2 foi obtido através do contrato atual do TRE-MS, com atualização do valor - R$ 62.357,30.

Preço 3 - O preço 3 foi obtido através de proposta enviada pela empresa SERVIX - R$ 103.437,000 (36 meses).

5.2 MAPA COMPARATIVO DOS CUSTOS TOTAIS DE PROPRIEDADE

Como apenas uma solução atende a necessidade da contratação, não há como comparar custos entre soluções.

6. DA ESCOLHA E JUSTIFICATIVA DA STIC ESCOLHIDA

6.1 DESCRIÇÃO DA SOLUÇÃO de TIC A SER CONTRATADA

Renovação das licenças da Ferramenta de Gestão de Vulnerabilidades (Tenable.sc) atualmente implantada no TRE-MS.

6.2 ALINHAMENTO DA SOLUÇÃO

A solução escolhida atende às necessidades de negócio quando contribui no alcance do objetivo estratégico "Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados", constante do PEI do TRE-MS. E, atende às necessidades de TI quando contribui para melhorar o objetivo estratégico "Aprimorar a Segurança da Informação e a Gestão de Dados" e o indicador "KR1- 7.1 - Número de vulnerabilidades críticas e altas", constantes do PDTIC do TRE-MS.

6.3 BENEFÍCIOS ESPERADOS

- Gerenciamento de vulnerabilidades, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral e Conformidade com normas de gestão de segurança da informação.

6.4 RELAÇÃO ENTRE A DEMANDA PREVISTA E A SER CONTRATADA

A demanda prevista é a renovação de 05 (cinco) Licenças da plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 250 endereços IP, por 36 meses de uso e suporte pelo fabricante e de 02 (duas) Licenças para solução de análise dinâmica em aplicações Web, pacote para no mínimo 5 domínios (FQDN), por 36 meses de uso e suporte pelo fabricante, conforme previsto no DOD e de acordo com a licitação realizada em 2020. Mas, o licenciamento fornecido pela empresa contratada pelo TRE-MS contempla em 05 (cinco) Licenças as licenças inicialmente pretendidas.

Durante a elaboração do Estudo Preliminar, a equipe de planejamento da contratação identificou essa situação de 2020 e optou apenas por 01 (um) item com as 05 (cinco) unidades contratadas em 2020.

6.5 ADEQUAÇÃO DO AMBIENTE

Não será necessária nenhuma adequação do ambiente.

6.6 ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Como a única solução verificada foi a contratação de uma empresa para renovação das licenças da solução de análise de vulnerabilidade já existente no TRE-MS (Tenable.sc), foi encontrada a média dos valores e o valor total da contratação ficou em R$ 384.490,50 (Trezentos e oitenta e quatro mil, quatrocentos e noventa Reais e cinquenta centavos).

7. SUSTENTAÇÃO DO CONTRATO

7.1 RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

7.1.1 RECURSOS MATERIAIS

Todos os Recursos Materiais necessários deverão ser fornecidos pela empresa contratada.

7.1.2 RECURSOS HUMANOS

Serão necessários 2 (dois) servidores do quadro para atuarem como fiscais do contrato.

7.2 ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

O serviço é de apenas uma execução, não há continuidade do serviço. Dessa forma, há somente entrega ou não do serviço contratado.

7.3 TRANSIÇÃO CONTRATUAL

Não se aplica porque não se trata de um serviço continuado.

7.4 ESTRATÉGIA DE INDEPENDÊNCIA TECNOLÓGICA

7.4.1 TRANSFERÊNCIA DE CONHECIMENTO

O uso da ferramenta já é de domínio dos servidores do TRE-MS, não havendo necessidade de transferência de conhecimento.

7.4.2 DIREITOS DE PROPRIEDADE INTELECTUAL

Não se aplica porque não se trata de um serviço continuado. É apenas o fornecimento de licenças de uso de software, prestação de serviço sob demanda.

7.5 CRITÉRIOS DE SUSTENTABILIDADE

- Os documentos e/ou relatórios deverão ser entregues, sempre que possível, por via informatizada de forma a não utilizar papel ou outro insumo semelhante;
- Caso a impressão seja necessária, a empresa deve adotar práticas de impressão sustentáveis, como a utilização de papel reciclado, impressão frente e verso e a minimização do uso de tintas prejudiciais ao meio ambiente;
- Este TRE, quando da redação da cláusula que estipula os horários de realização dos serviços, deu preferência por conciliar com horários de funcionamento do órgão onde a energia e demais insumos já são utilizados.

8. ESTRATÉGIA PARA A CONTRATAÇÃO

8.1 NATUREZA DO OBJETO

Trata-se de contratação de serviços Comuns de Tecnologia da Informação, se submetendo à resolução CNJ 468/2022.

8.2 PARCELAMENTO DO OBJETO

Não é viável o parcelamento do objeto por se tratar de renovação das licenças da solução de análise de vulnerabilidades.

8.3 ADJUDICAÇÃO DO OBJETO

O objeto da contratação será adjudicado por uma única empresa.

8.4 MODALIDADE E TIPO DE LICITAÇÃO

A contratação da renovação das licenças será realizada mediante licitação na modalidade de PREGÃO, em sua forma eletrônica, no do tipo menor preço, nos termos do inciso XLI, art 6º e art. 29 da da Lei 14.133/2021

> art. 6º [...]
>
> XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;
>
> [...]
>
> art. 29. A concorrência e o pregão seguem o rito procedimental comum a que se refere o art. 17 desta Lei, adotando-se o pregão sempre que o objeto possuir padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado. (*grifo nosso)*

No presente caso, não será adotado Sistema de Registro de Preços.

8.5 CLASSIFICAÇÃO E INDICAÇÃO ORÇAMENTÁRIA

As despesas decorrentes do objeto desta licitação, serão custeadas com recursos aprovados pela Lei Orçamentária da União nº 14.535 de 17/01/2023, que estima a receita e fixa a despesa da União para o exercício financeiro 2023 (LOA), Unidade 14112 – TRE-MS, Ação: 20GP – Julgamento de Causas e Gestão Administrativa, Programa de Trabalho 02.122.0033.20GP.0054, Elementos de Despesa: 3390.40.07 - Manutenção Corretiva/Adaptativa e Sustentação de Software.

As despesas que vierem a ocorrer nos exercícios futuros serão custeadas com recursos previstos nas respectivas Propostas Orçamentárias, e serão indicados oportunamente.

As informações acerca da disponibilidade orçamentária podem ser alterados pela COPEG.

8.6 VIGÊNCIA DA PRESTAÇÃO DE SERVIÇO

O período de vigência desta contratação será de 36 (trinta e seis) meses. O prazo para início da execução será após o vencimento da validade das licenças, qual seja 23/12/2023.

O período de 36 (trinta e seis) meses se deve ao período de validade das licenças. O contrato sendo de um tempo maior, o preço tende a diminuir, conforme proposta apresentada pela empresa SERVIX para 36 meses e 60 meses. Para 36 meses, o valor mensal da solução fica R$ 2.873,25 e para 60 meses o valor diminui para R$ 2.819,42. Uma redução de R$ 53,83/mês/licenças, R$ 269,15/mês e R$ 3.229,80/ano.

8.7 EQUIPE DE APOIO À CONTRATAÇÃO (Art. 20 Resol. 468 CNJ)

A equipe que subsidiará a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes pertence à Secretaria de Tecnologia da Informação e os servidores encontram-se lotados no Gabinete da STI, Antônio Mendes Barata Segundo, na Coordenadoria de Infraestrutura de Tecnologia da Informação e Suporte, Marcelo Silva de Novaes e na SAF/Coordenadoria de Recursos Materiais/SLC, pela servidora Edismar Martins da Silva Lima.

8.8 EQUIPE DE GESTÃO DA CONTRATAÇÃO (Arts. 21e 24 Resol. 468 CNJ)

- Gestor da contratação: Luciana J. V. de Aguiar
- Fiscal demandante: Antônio Mendes Barata Segundo
- Fiscal técnico: Ulysses Pereira de Almeida Neto
- Fiscal administrativo: a ser indicado pela Secretaria de Administração e Finanças

8.9 OBRIGATORIEDADE DE EXIGÊNCIA DE CONTRATAÇÃO DE EGRESSOS

Não aplicável.

Não há alocação de mão de obra na presente contratação, conforme exige a Resolução CNJ 307/2019, não haverá necessidade de profissionais da contratada no local de prestação dos serviços.

8.10 ATESTADO DE CAPACIDADE TÉCNICA (quando aplicável)

Não se aplica.

8.11. Consórcio: Tendo em vista o valor da contratação, a baixa complexidade do objeto e o ramo de mercado a atender a demanda, não será admitido a participação de consórcio na presente contratação.

8.12. Garantia: Não haverá exigência de garantia dos artigos 96 e seguintes da Lei nº 14.133, de 2021.

8.13. Amostra*:* Não haverá exigência de apresentação de amostra.

9. ANÁLISE DE RISCOS

O Mapa de Gerenciamento de Riscos foi produzido pela equipe de planejamento e está registrado no processo sob ID nº 1507378.

10. DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

A equipe de planejamento, diante dos dados expostos, entende que a contratação é viável e necessária, para manutenção da gestão de vulnerabilidades das aplicações e infraestrutura de TI do TRE-MS.

ANTÔNIO MENDES BARATA SEGUNDO
Integrante Demandante

MARCELO SILVA DE NOVAES
Integrante Técnico

GRAZIELA GONÇALVES SILVA JURADO
Integrante Administrativa

Documento assinado eletronicamente por **GRAZIELA GONÇALVES SILVA JURADO**, **Chefe de Seção**, em 09/10/2023, às 15:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCELO SILVA DE NOVAES**, **Coordenador(a)**, em 10/10/2023, às 10:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANTÔNIO MENDES BARATA SEGUNDO**, **Técnico Judiciário**, em 16/10/2023, às 12:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1482244** e o código CRC **60BB93D3**.