TERMO DE REFERÊNCIA

ANEXO I

Processo Administrativo nº 0004039-54.2023

Referência: Resolução CNJ 468/2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação do suporte das licenças da Ferramenta de Gestão de Vulnerabilidades atualmente implantada no TRE-MS.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO (36 meses)	VALOR TOTAL (36 meses)	Intervalo mínimo entre os lances
1	Renovação de Subscrição Tenable (TSCCV-P e TSCCV-M) pelo período de 36 (trinta e seis) meses	15741	Unidade	05	R$ 76.898,10	R$ 384.490,50	R$ 10,00

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comuns**, uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

1.3. O prazo de vigência da contratação é de 38 (trinta e oito) meses, contados da assinatura do contrato e o prazo para início da execução será de 15 (quinze) dias, contados do recebimento da nota de empenho, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

2.1. ITEM 1 - Renovação de Subscrição Tenable (TSCCV-P e TSCCV-M) pelo período de 36 (trinta e seis) meses.

Requisitos gerais

2.1.1. 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;

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

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

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

2.1.5. 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;

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

2.1.7. 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;

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

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

2.1.10. Deve possuir um sistema de busca de informações de um determinado ativo com no mínimos as seguintes características:
2.1.10.1. Por sistema operacional;
2.1.10.2. Por um determinado software instalado;
2.1.10.3. Por Ativos impactados por uma determinada vulnerabilidade.

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

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

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

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

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

2.1.16. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
2.1.16.1. CVSSv3 Impact Score;
2.1.16.2. Idade da Vulnerabilidade;
2.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;
2.1.16.4. Número de produtos afetados pela vulnerabilidade;

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

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

2.1.19. 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;

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

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

2.1.22. 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;

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

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

2.1.25. 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;

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

2.1.27. 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;

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

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

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

2.1.31. 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.

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

2.1.33. 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).

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

2.1.35. Dos Relatórios:
2.1.35.1. Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
2.1.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
2.1.35.3. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;
2.1.35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;
2.1.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
2.1.35.6. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
2.1.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
2.1.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

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

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

2.1.37.1. Hosts verificados sem credenciais;
2.1.37.2. Top 100 Vulnerabilidades mais criticas;
2.1.37.3. Top 10 Hosts infectados por Malwares;
2.1.37.4. Hosts exploráveis por Malwares;
2.1.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
2.1.37.6. Vulnerabilidades críticas e exploráveis;
2.1.37.7. Máquinas com vulnerabilidades que podem ser exploradas;

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

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

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

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

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

2.1.43. Deve ser capaz de medir e reportar ameaças;

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

2.1.45. 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;

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

2.1.47. 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;

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

2.1.49. 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.

2.1.50. 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;

2.1.51. 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;

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

2.1.53. 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;

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

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

2.1.56. 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;

2.1.56.1. 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;
2.1.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;
2.1.56.3. A solução de análise deverá ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);
2.1.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;
2.1.56.5. 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;

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

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

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

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

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

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

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

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

2.1.56.14. 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;

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

2.1.56.16. Deve suportar o envio de notificações por email;

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

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

a) Autenticação Básica (Digest);
b) NTLM;
c) Autenticação de Cookies;

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

2.1.56.20. 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;

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

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

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

2.1.56.24. 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.

2.1.57. 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).

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A solução permitirá a substituição e teste da funcionalidade dentro de prazos adequados que não impactem a disponibilidade do datacenter container.

3.2. A atual demanda ordinária da contratação do serviço para Justiça Eleitoral do Mato Grosso do Sul inclui, mas não se limita, a:

3.2.1. 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.

3.3. O objeto da contratação está previsto no Plano de Contratação Anual 2023, conforme Processo SEI 0009204-19.2022.6.12.8000 (Documento 1440787), publicado na página deste TRE/MS na internet.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos Legais

4.2.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021 (Pesquisa de preços), Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Resolução CNJ 468/2022 e a outras legislações aplicáveis.

4.2. Sustentabilidade

4.2.1. A CONTRATADA deverá adotar as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:

4.2.1.1. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

4.2.1.2. Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

4.2.1.3. Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de

forma a garantir a máxima proteção durante o transporte e o armazenamento;

4.2.1.4. Que sejam utilizados produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;

4.2.1.5. Os documentos e/ou relatórios deverão ser entregues, sempre que possível, por via informatizada de forma a não utilizar papel ou outro insumo semelhante;

4.2.1.6. Caso a impressão seja necessária, a contratada 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;

4.2.1.7. 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.

4.2.1.8. As embalagens a serem utilizadas na realização dos serviços, sempre que possível, deverá ser de material de baixo impacto ecológico.

4.2.1.9. A empresa contratada deverá fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços.

4.3. Não é admitida a subcontratação do objeto contratual.

4.4. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.4.1. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações do CONTRATANTE:

5.1.1. requisitar a prestação dos serviços, na forma prevista neste Termo de Referência;

5.1.2. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.3. encaminhar formalmente a demanda por meio e-mail, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.4. exigir da CONTRATADA o fiel cumprimento das obrigações decorrentes desta contratação;

5.1.5. receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.6. verificar a manutenção pela CONTRATADA das condições de habilitação estabelecidas na licitação;

5.1.7. aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

5.1.8. liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

5.1.9. comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.10. Efetuar o pagamento à CONTRATADA, de acordo com as condições de preço e prazo estabelecidos neste Termo de Referência;

5.1.11. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

5.1.12. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações da CONTRATADA

5.2.1. Realizar a prestação do serviço decorrente desta contratação na forma e condições

determinadas no Edital e neste Termo de Referência (Anexo I).

5.2.2. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.3. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.4. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.5. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.6. Manter, durante todo o prazo de execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na fase de habilitação da licitação.

5.2.7. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.8. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.9. Assumir todos os encargos de possível demanda trabalhista, cível ou penal relacionada à prestação do serviço, sendo de inteira responsabilidade do contratado a contratação de funcionários necessários à perfeita execução do fornecimento.

5.2.10. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.11. Receber os valores que lhe forem devidos pela prestação dos serviços, na forma disposta neste Termo de Referência.

5.2.12. Fazer a transição contratual, quando for o caso;

5.2.13. Abster-se de praticar atos ilícitos, em especial os descritos no artigo 5º da Lei Federal nº 12.846, de 2013, bem como observar os princípios da legalidade, moralidade, probidade, lealdade, confidencialidade, transparência, eficiência e respeito aos valores preconizados no Código de Conduta Ética do TRE/MS (Resolução 690/2020).

5.2.14. Dar plena ciência do disposto na Portaria Direção-geral nº 176/2023 TRE/PRE/DG/GABDG, a qual dispõe sobre os procedimentos para apuração e aplicação de penalidades decorrentes do descumprimento de regras licitatórias e/ou obrigações contratuais decorrentes da Lei nº 14.133, de 1º de abril de 2021, no âmbito do Tribunal Regional Eleitoral de Mato Grosso do Sul.

5.2.15. Dar conhecimento, aos funcionários de seus respectivos quadros que participarão da execução contratual, sobre o Código de Conduta Ética do TRE/MS para ciência e responsabilidade em sua observância.

5.2.15.1. O mesmo se aplica à subcontratada (se for o caso).

5.2.16. Proteger informações confidenciais e privilegiadas, conforme regulamento próprio.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Os serviços serão prestados no prédio-sede do TRE-MS, sito na Rua Desembargador Leão Neto do Carmo, nº 23, Parque dos Poderes, Campo Grande-MS.

6.1.1. A empresa deverá, no horário das 12:00h as 18:00h (preferencialmente), de segunda à sexta-feria, através do telefone (67) 2107- 7123 com Clodoaldo Fonseca e Ulysses Neto, agendar a entrega.

6.2. O PRAZO MÁXIMO para início da execução é o vencimento da validade do suporte das licenças, qual seja 23/12/2023.

6.3. Não será necessária transferência de conhecimento devido às características do objeto.

6.4. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

6.5. Manutenção de Sigilo e Normas de Segurança

6.5.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.5.2. O modelo de Termo de Compromisso de Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, e T ermo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS I-B e I-C".

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.3.1. A fiscalização, acompanhamento e a orientação relativa à prestação dos serviços/fornecimento ficarão a cargo de servidor pertencente ao quadro deste Tribunal.

7.3.2. O contato entre este Tribunal e a empresa contratada será mantido, prioritariamente, por intermédio da fiscalização

7.4. O órgão poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato, quando for o caso.

7.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), observando-se, em especial, as rotinas a seguir:

7.5.1. Acompanhar a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.5.2. Identificada qualquer inexatidão ou irregularidade, a fiscalização emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.5.3. Informar à administração, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.5.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

7.5.5. Comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.6. Verificar a manutenção das condições de habilitação da CONTRATADA, acompanhar o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.6.1. Atuar tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a competência do fiscal; (Decreto nº 11.246, de 2022, art. 23, IV).

7.6.2. manter registro de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.6.3. formalizar processo administrativo de responsabilização para fins de aplicação de

sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.6.4. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

7.6.5. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.6.5.1. requisitar a prestação dos serviços e/ou fornecimento, mediante Ofício ou Requisição de fornecimento;

7.6.5.2. exercer, em nome do Tribunal Regional Eleitoral, toda e qualquer ação de orientação geral, decidir sobre questões técnicas e burocráticas dos serviços, sem que isto implique em transferência de responsabilidade, a qual será única e exclusivamente de competência da CONTRATADA.

7.6.5.3. conferir e atestar a Nota Fiscal/Fatura emitida pela empresa contratada, encaminhando-a para pagamento;

7.6.5.4. outras atribuições pertinentes à contratação ou que lhe forem conferidas pela Administração.

8. CRITÉRIOS DE MEDIÇÃO PARA PAGAMENTO

Do recebimento

8.1. O recebimento provisório será realizado pela fiscalização (STI), no prazo de 02 (dois) dias, compreendendo, dentre outras, as seguintes verificações:

8.1.1. apresentação do documento fiscal, com identificação do fornecedor e do comprador (TRE/MS), descrição do serviço, quantidade, preços unitário e total; e

8.1.2. compatibilidade dos serviços entregues com as especificações exigidas neste Termo de Referência e constantes da proposta da empresa.

8.2. Atendidas as condições indicadas na cláusula acima, será registrado o recebimento provisório mediante atestado no verso da Nota Fiscal, ou, em termo próprio.

8.2.1. O atestado de recebimento registrado em canhoto de nota fiscal, ou documento similar, não configura o recebimento definitivo do material.

8.3. O prazo constante na cláusula 8.1. será contado do recebimento de comunicação de cobrança oriunda da CONTRATADA com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.4. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução dos serviços.

8.5. A fiscalização não efetuará o ateste dos serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).

8.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.7. Os serviços serão recebidos definitivamente no prazo de 05 (cinco) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado.

8.8. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

8.9. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.10. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela CONTRATADA, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.11. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9. DA LIQUIDAÇÃO

9.1. A Nota Fiscal/Fatura deverá ser emitida, preferencialmente, em meio eletrônico e conter a indicação do serviço prestado, conforme a discriminação da Nota de Empenho, quantidade, e os preços unitário e total.

9.2. Para fins de atendimento a IN/RBF 1.234, de 11/01/2012 (alterada pela IN/RBF nº 1.244/2012), a empresa deverá informar no documento fiscal os valores detalhados das contribuições federais a serem retidos na operação, exceto se a empresa for OPTANTE PELO SIMPLES.

9.3. O procedimento de pagamento da Nota Fiscal só se efetivará após o Recebimento Definitivo e mediante a comprovação da existência de conta bancária válida e ativa em nome da empresa, além da regularidade fiscal (INSS/FGTS), trabalhista e manutenção das demais condições de habilitação exigidas no edital.

9.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a CONTRATADA providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE.

9.5. Constatando-se situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

9.5.1. A permanência da condição de irregularidade, sem a devida justificativa ou com justificativa não aceita pela Administração, pode culminar em rescisão contratual, sem prejuízo da apuração de responsabilidade e da aplicação de penalidades cabíveis, observado o contraditório e a ampla defesa.

9.5.2. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

9.6. É facultada a retenção dos créditos decorrente do contrato, até o limite dos prejuízos causado à Administração Pública e das multas aplicadas, nos termos do inciso IV do art. 139 da Lei nº 14.133, de 2021.

10. PRAZO DE PAGAMENTO

10.1. O pagamento será mensal e efetuado no prazo de até 07 (sete) dias úteis, contados do recebimento definitivo do objeto pela fiscalização, por meio de ordem bancária, para crédito em banco, agência e conta corrente válida e em nome da empresa, indicados pela CONTRATADA.

10.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

10.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

10.3.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

a) Imposto de Renda, Contribuição Social Sobre Lucro Líquido-CSLL, COFINS e PIS/PASEP, nos termos da Lei 9.430/96, salvo opção da empresa pelo SIMPLES – Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e empresas de Pequeno Porte, hipótese em que o fornecedor deverá comprovar a Opção;

b) Imposto Sobre Serviços de Qualquer Natureza – ISSQN, se este for devido.

10.4. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida LeiComplementar.

10.5. Em caso de atraso no pagamento por parte do Tribunal, os valores a serem pagos serão atualizados, desde a data final do período de adimplemento de cada parcela até a data do efetivo pagamento, mediante a aplicação da seguinte fórmula: EM = I x N x VP, onde: EM = Encargos

Moratórios; N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela em atraso; I = Índice de compensação financeira = 0,00016438, assim apurado: i = taxa percentual anual do valor de 6%, I = i / 365 → I = (6/100) / 365.

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

11.2. O regime de execução do contrato será por empreitada por preço unitário.

11.3. Será dado direito de preferência previsto na Lei Complementar n.º 123/2006 à licitante microempresa ou empresa de pequeno porte que tenha declarado seu enquadramento como tal.

11.4. A análise técnica das propostas, será realizada pelos integrantes da equipe responsável pelo planejamento da contratação (integrante da área demandante e/ou integrante técnico) e visa à verificação da conformidade dos serviços ofertados pelas licitantes com as especificações indicadas neste Termo de Referência.

11.5. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

a. CERTIDÃO CONJUNTA NEGATIVA DE DÉBITOS RELATIVOS A TRIBUTOS FEDERAIS E A DÍVIDA ATIVA DA UNIÃO, administrados pela Secretaria da Receita Federal, devidamente válida, constando expressa a abrangência das contribuições sociais previstas nas alíneas “a” a “d” do parágrafo único do art. 11 da Lei nº 8.212 de 24 de julho de 1991;

b. CERTIDÃO DE REGULARIDADE DO FGTS (CRF), devidamente válida, emitida pela Caixa Econômica Federal, que comprove inexistência de débito perante o FGTS;

c. CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS (CNDT), devidamente válida, emitida pela Justiça do Trabalho nos termos do Título VII-A da Consolidação das Leis do Trabalho;

d. Declaração de que a empresa não utiliza menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre; nem menores de 16 (dezesseis) anos para qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos, em conformidade ao disposto no inciso XXXIII, do artigo 7º da Constituição Federal, em campo próprio do sistema.

e. CERTIDÃO DE FALÊNCIA - CERTIDÃO NEGATIVA DE FEITOS SOBRE FALÊNCIA,RECUPERAÇÃO JUDICIAL E RECUPERAÇÃO EXTRAJUDICIAL, expedida peloDistribuidor da sede da Pessoa Jurídica;

e.1. A apresentação de certidão positiva de feitos sobre recuperação judicial e extrajudicialnão ensejará a imediata inabilitação do licitante. A empresa que se encontrar em recuperação judicial/extrajudicial deverá apresentar, juntamente com a certidão positiva, a comprovação de que seu plano de recuperação foi aprovado e homologado judicialmente, com a recuperação já deferida.
e.2. A certidão em que não constar prazo de validade, será atribuída validade de 90(noventa) dias, contados da data de emissão.

.

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

12.1. O custo estimado da contratação é de R$ 384.490,50 (Trezentos e oitenta e quatro mil, quatrocentos e noventa Reais e cinquenta centavos), para 36 (trinta e seis) meses, conforme custos unitários apostos no mapa comparativo de preços.

12.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre CONTRATANTE e CONTRATADA, conforme especificado na matriz de risco.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

13.2. A contratação será atendida pela seguinte dotação:

a) Gestão/Unidade: 14112 – TRE-MS;

b) Fonte de Recursos: : 21EE – Gestão da Política de Segurança da Informação e Cibernética na Justiça Eleitoral;

c) Programa de Trabalho: 02.122.0033.21EE.0001;

d) Elemento de Despesa: 3390.40.07- PLANO INTERNO TIC MANSOF

13.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. As disposições quanto as infrações e sanções administrativas estão previstas no Anexo II - Termo de Contrato Administrativo.

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 22/11/2023, às 12:40, 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 **1542858** e o código CRC **870623B7**.