

**TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA**

Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58013-251 - João Pessoa - PB - <http://www.tre-pb.jus.br>

Termo de Referência de Serviços de TIC nº 1904605 - TRE-PB/PTRE/DG/STIC/COESC/SESEC**1. Definição do objeto (Art. 6º, XXIII, "a", da Lei nº 14.133/2021):**

O presente Termo de Referência tem como objeto a contratação de empresas especializadas no fornecimento de uma solução de filtragem de e-mails para atender as necessidades do Tribunal Regional Eleitoral da Paraíba, conforme discriminação abaixo:

Item	CATSER	Descrição	Quantidade
01	27502	Subscrição Solução para filtragem de e-mail para 2.000 caixas de e-mail, com suporte do fabricante, por 36 (trinta e seis) meses e com pagamento em parcela única	1
02	26972	Instalação e Configuração da Solução	1
03	26972	Repasse tecnológico de no mínimo 20h para 10 alunos	1
04	26972	Suporte técnico Especializado por 36 (trinta e seis) meses 24x7 (24 horas/dia e 7 dias/semana) com pagamento em parcela única	1

Quanto à natureza do serviço, constata-se que, conforme artigo 6º, XIII e XV, da Lei nº 14.133/2021, ele é considerado contínuo, uma vez que a sua descontinuidade pode gerar prejuízo a segurança da informação do serviço de correio eletrônico do TRE-PB.

O prazo de vigência da contratação é de 36 meses, contados da última assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133/2021, tendo em vista o seu caráter de serviço continuado, sendo mais vantajosa a vigência plurianual, considerando que, se a execução contratual estiver sendo exitosa, se houver orçamento e se o preço contratado coadunar-se com o de mercado, não há razão

para se lançar outra licitação, onde há até o risco de não ser Contratada empresa com gestão interna que proporcione uma execução contratual bem-sucedida.

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

2. Fundamentação da contratação (Art. 6º, XXIII, "b", da Lei nº 14.133/2021):

A fundamentação desta contratação e de seus quantitativos encontra-se pormenorizada nos Estudos Técnicos Preliminares executados (1935329).

Esta contratação está prevista nos seguintes documentos:

- [Plano de Contratações de Soluções de TIC 2024](#) - Item 35;
- [Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário \(ENTIC-JUD\)](#) - Objetivo 1,2 e 7
- [Plano Estratégico do TRE-PB](#) - Objetivo 8.

3. Descrição da solução como um todo, considerando todo o ciclo de vida do objeto (Art. 6º, XXIII, "c", da Lei nº 14.133/2021):

Com a necessidade cada vez mais premente de aumentarmos os investimentos em segurança e ampliarmos o leque de prevenção à superfície de ataques no nosso servidor de e-mail, a aquisição de ferramenta para filtragem de mensagens indesejadas (especialmente spams e phishing), ajudará nesse desiderato através da prevenção proativa de incidentes de segurança em nosso ambiente envolvendo os diversos tipos de tentativa de invasão através da plataforma de e-mail, diminuindo consideravelmente as mensagens falsas, que além de representarem um elevado risco à Segurança da Informação, podem comprometer os dados institucionais, sendo de extrema importância a presente aquisição visando a proteção contra esses potenciais problemas.

4. Requisitos da contratação (Art. 6º, XXIII, "d", da Lei nº 14.133/2021):

4.1. Instrumento de contrato:

4.1.1 Deverá ser celebrado instrumento formal de contrato diante das peculiaridades e das necessidades desta contratação.

4.2. Subcontratação:

4.2.1 Somente será possível a subcontratação para os itens 02 (Instalação) , 03 (Repasse Tecnológico) e 04 (Suporte Especializado), desde que expressamente autorizada pela Administração.

4.2.2 De acordo com o artigo 122, §3º, da Lei nº 14.133/2021, será vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade Contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

4.2.3 O contrato oferece maior detalhamento das regras que serão aplicadas em relação à subcontratação.

4.3. Participação de consórcios e pessoa física:

4.3.1 A formação de consórcios traz consigo um maior custo administrativo para a futura equipe de gestão e fiscalização do contrato. Dessa forma, não se faz necessária a junção de empresas para a perfeita execução do objeto, ao mesmo tempo em que amplia sobremaneira a competitividade do certame.

4.3.2 No que concerne à pessoa física, considerando que esta contratação exigirá capital social mínimo e estrutura mínima, com equipe de profissionais para a execução do objeto, verifica-se ser incompatível a execução do objeto por pessoa física, nos termos do [artigo 4º, parágrafo único, da Instrução Normativa n. 116/2021-SEGES/ME](#).

4.4. Requisitos legais:

4.4.1 O presente processo de contratação está aderente à Constituição Federal, à [Lei nº 14.133/2021](#), à Instrução Normativa SGD/ME nº 94, de 2022, à Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, à [Instrução Normativa nº 05/2017 - SEGES/MPDG](#), à [Lei nº 13.709/2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD), à Lei nº 9.609/98 (dispõe sobre a proteção da propriedade intelectual de programa de computador), ao [Decreto nº 9.507/2018](#), ao [Decreto nº 7.174/2010](#), ao [Decreto nº 11.246/2022](#), à [Resolução nº 468/2022-CNJ](#), à [Resolução nº 443/2022 - CNJ](#), à [Resolução nº 335/2020 - CNJ](#), à [Portaria nº 257/2022 - CNJ](#), à [Portaria nº 750/2023 - SGD/MGI](#) e à [Resolução nº 23.702/2022 - TSE](#).

4.5. Requisitos temporais:

4.5.1 Prazo de entrega da solução: até 15 (quinze) dias corridos a partir da data da assinatura do contrato, prorrogáveis por interesse e/ou conveniência da administração;

4.5.1.1 No caso de appliance físico o Prazo de entrega da solução: até 60 (sessenta) dias corridos a partir da data da assinatura do contrato, prorrogáveis por interesse e/ou conveniência da administração;

4.5.1.2 O prazo de instalação é de até 10 (dez) dias corridos a partir da entrega da solução. Isso inclui deixar a solução em perfeito funcionamento com todas as funções previstas no presente Termo de Referência;

4.5.1.3 O recebimento provisório será dado no dia da conclusão da instalação segundo as funções previstas no presente Termo de Referência.

4.5.2 Devem ser fornecidos com ou sem a mídia de instalação. No caso de não fornecimento de mídia, deve ser indicado local para download do arquivo de instalação;

4.5.3 Devem ser apresentados chave única tipo serial ou qualquer outra forma de validação da ferramenta, comprovando perante o fabricante que trata-se de uma ferramenta devidamente licenciada;

4.5.4 O atraso não justificado deverá ser punido de acordo com as sanções aplicadas ao contrato.

4.6. Requisitos de segurança da informação:

4.6.1 A Contratada deverá manter sigilo em relação aos dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como se submeter às orientações e normas internas de segurança da informação vigentes, devendo orientar seus empregados e/ou preposto nesse sentido.

4.6.2 A Contratada cumprirá, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

4.6.3 Pertencerão exclusivamente ao Contratante os direitos relativos aos produtos desenvolvidos e elaborados para a prestação do objeto, sendo vedada sua reprodução, transmissão e/ou divulgação sem o seu respectivo consentimento.

4.6.4 Em caso de desligamento/afastamento de qualquer empregado/prestador de serviço da Contratada, esta deverá comunicar imediatamente ao Contratante, que deverá revogar todos os acessos aos sistemas/serviços.

4.6.5 Tendo em vista que a solução a ser Contratada lidará com ativos de informação de alto risco, conforme disposto no [artigo 3º, I, da Instrução Normativa nº 02/2021-TRE/PB](#), a futura Contratada e seus profissionais deverão assinar o Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB e a Declaração de Ciência do Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB, respectivamente, cujos modelos seguem no item 10.

4.7. Requisitos de evolução tecnológica:

4.7.1 Deve a Contratada garantir a atualização tecnológica de sua equipe para a prestação dos serviços.

4.7.2 A capacitação dos novos profissionais é parte integrante do processo seletivo de responsabilidade da Contratada, sendo realizado após o recrutamento e seleção, e deverá ser aplicada de acordo com perfil definido do profissional alocado nos serviços de

desenvolvimento e de manutenção de sistemas.

4.7.3 Todos os custos relacionados aos treinamentos dos novos profissionais da Contratada que vierem a prestar serviços à Contratante serão de responsabilidade da Contratada, sem nenhum ônus adicional à Contratante, devendo tais treinamentos serem realizados nas dependências da própria Contratada ou onde for de sua conveniência.

4.7.4 Com vistas à manutenção da excelência e ao aperfeiçoamento da prestação dos serviços, a Contratada, sem custos adicionais para a Contratante, deverá promover o constante desenvolvimento e capacitação de todos os integrantes da equipe, com foco em aspectos técnicos, comportamentais, motivacionais e de relacionamento com usuários.

4.7.5 Os treinamentos dos técnicos da Contratada, igualmente, deverão ser realizados de modo a garantir os níveis mínimos de serviço acordados, bem como atualizar estes técnicos quando da inclusão e atualização das plataformas de desenvolvimento de sistemas no ambiente de TIC da Contratada que exijam novas capacitações.

4.8. Requisitos não funcionais:

4.8.1 Devido à abrangência da contratação, que envolve manutenção de sistemas legados com requisitos e arquiteturas distintas, não se faz possível esgotar neste instrumento um conjunto suficiente de requisitos não funcionais. Assim, a Contratada deverá, durante o processo de abertura da solicitação de serviço, receber os requisitos solicitados. Entretanto, alguns desses podem ser estabelecidos de imediato. São eles:

1. Aderência às normas e padrões internos de procedimentos técnicos adotados pelo TRE-PB;
2. Respeito às normas de Segurança da Informação vigentes no TRE-PB;
3. Respeito ao Código de Ética do TRE-PB

4.9. Requisitos de sustentabilidade da solução:

4.9.1 A Contratada deve respeitar a legislação trabalhista vigente, observando que não será estabelecido qualquer vínculo empregatício ou de responsabilidade entre os profissionais que empregar para a execução dos serviços contratados e a Contratante.

4.9.2 A Contratada deve respeitar o direito de livre associação e negociação coletiva de seus empregados.

4.9.3 A Contratada deve respeitar e promover a diversidade, abstendo-se de todas as formas de preconceito e discriminação, de modo que nenhum empregado ou potencial empregado receba tratamento discriminatório em função de sua raça, cor de pele, origem étnica, nacionalidade, posição social, idade, religião, gênero, orientação sexual, estética

peçoal, condição física, mental ou psíquica, estado civil, opinião, convicção política, ou qualquer outro fator de diferenciação.

4.9.4 A Contratada deve coibir o assédio sexual e moral em sua força de trabalho.

4.9.5 A Contratada deve proteger e preservar o meio ambiente, bem como evitar quaisquer práticas que possam lhe causar danos, executando seus serviços em estrita observância às normas legais e regulamentares, federais, estaduais ou municipais, aplicáveis ao assunto, orientando seus empregados a observar atitudes sustentáveis, que sejam ambientalmente corretas, economicamente viáveis e socialmente justas. Todos os empregados devem ter conhecimento das práticas e programas de sustentabilidade da Contratante, observando e propagando princípios de TI Verde, dentre outros.

4.11. Termos a serem assinados pelo futuro contratado:

4.11.1 Para a prestação dos serviços, considerando as informações às quais os profissionais terão acesso, deverão ser assinados tanto por estes, como pelo representante legal da Contratada, os seguintes termos:

- Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB e
- Declaração de Ciência do Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB.

4.12. Especificações Técnicas da Solução de filtragem - Item 01 :

A solução oferecida engloba os itens acima e deverá ser obrigatoriamente implementada em appliance(s) físicos ou virtual appliance(s) ou como um Software/Serviço instalado em Sistema Operacional de máquinas virtuais do ambiente de virtualização do TRE-PB ou baseada em nuvem a ser(em) fornecido(s) pela Contratada.

4.12.1. Requisitos mínimos de software:

4.12.1.1. Ser um MTA completo com suporte ao protocolo SMTP, com registro de logs das atividades do MTA;

4.12.1.2. Possuir filtros de reputação;

4.12.1.3. Possuir solução antiphishing integrada;

4.12.1.4. Efetuar varredura de conteúdo (na entrada e na saída do correio eletrônico);

4.12.1.5. Possuir módulo de consulta customizada e impressão de relatórios estatísticos;

4.12.1.6. Possuir a funcionalidade de SPF;

4.12.1.7. Possuir a funcionalidade de DKIM;

4.12.1.8. Possuir a funcionalidade de DMARC;

4.12.1.9. Possuir a funcionalidade de RBL;

4.12.1.10. Possuir capacidade de bloquear acesso a URLs maliciosa;

4.12.1.11. Possuir capacidade de detecção e bloqueio de malwares (na entrada e na saída do correio eletrônico);

4.12.1.12. As mensagens recebidas com links e não classificadas como maliciosa (spam, phishing, malware) deverão ter os links da mensagem reescritos para que possam ter a sua reputação avaliada pela solução no momento do click do usuário no link da mensagem.

4.12.2. Requisitos mínimos de disponibilidade e performance:

4.12.2.1 Deve ser entregue pronta para alta disponibilidade contando com, no mínimo, 2 **(dois)** pontos de acesso (nós) funcionando em ativo-ativo ou ativo-passivo desde que atenda a capacidade de proteção de 2.000 caixas de email;

4.12.2.2 Eventuais licenças necessárias às funcionalidades pretendidas na presente aquisição devem necessariamente estar inclusas na solução;

4.12.2.3 A solução deve suportar cluster de Alta Disponibilidade na forma de Cluster Ativo-Ativo com Balanceamento de carga ou Ativo-Passivo com Fail Over automático através do registro MX, assegurando que as funções de filtragem , serviço de recebimento, processamento e entrega das mensagens não pare por falha na solução;

4.12.2.4 A criação e configuração do Cluster deve ser efetuada através da interface gráfica do gerenciador da solução, ou por linha de comando da solução;

4.12.2.5 Possuir capacidade de replicação automática das configurações através da gerência por enderçamento IP

4.12.2.6 A inclusão de novos nodes no cluster deve ser possível para garantir a escalabilidade da solução de forma simplificada ou deve ser efetuado através da interface gráfica de gerenciamento (GUI), sem necessidade de utilização de linhas de comando;

4.12.3. Interfaces para o Administrador:

4.12.3.1. Todos os requisitos descritos no item deverão ser consolidados em interfaces gráficas e de textos;

4.12.3.2. A interface gráfica deverá permitir acesso via HTTPS;

4.12.3.3. A mesma interface deverá gerenciar todos os produtos instalados na solução;

4.12.3.4. Deve possuir administração via shell, através de SSH para CLI (command line interface), para execução de comandos de administração e suporte;

4.12.4. O sistema deve permitir a integração nativa com os principais sistemas de colaboração do mercado, entre eles:

4.12.4.1. Microsoft Exchange®;

4.12.4.2. Zimbra Collaboration Suite®;

4.12.5. A solução não pode ser intrusiva, devendo ser instalada facilmente sem modificar a estrutura da rede DMZ, no caso de virtual appliance;

4.12.6. A solução deverá possuir a capacidade de criação e gerenciamento de múltiplos grupos de usuários e a definição de regras e políticas diferenciadas para cada um destes grupos;

4.12.7. Da compatibilidade:

4.12.7.1 Se a solução for ofertada como appliance virtual, deve ser compatível com todos os principais sistemas de virtualização do mercado, entre eles: Nutanix AHV, VMWare e Microsoft Hyper-V;

4.12.7.2 Se a solução for ofertada como software/serviço instalado em Sistema Operacional de máquinas virtuais do ambiente de virtualização do TRE-PB, deve ser compatível com Windows Server Datacenter ou Red Hat Enterprise Linux ;

4.12.8 Deve possuir mecanismo de backup e recuperação da configuração da solução na própria interface gráfica do produto, sem necessidade de linha de comando;

4.12.9 Deve possuir capacidade de envio de backup automático da configuração via FTP ou SFTP ou SMB, sendo configurado diretamente na interface gráfica da solução (sem necessidade de qualquer configuração em linha de comando);

4.12.10 Deve possibilitar manter na própria ferramenta o backup da configuração da solução por período mínimo de 90 dias, possibilitando recuperação do mesmo a qualquer momento;

4.12.11 Deve possuir banco de dados para armazenamento dos registros de acesso, logs de sistema e configurações. Caso a solução necessite de banco de dados específico e proprietário, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante. Não serão aceitas soluções baseadas em armazenamento de Logs em formato Texto;

4.12.12 Deve possuir sistema de diagnóstico via interface WEB ou Console, com no mínimo a execução dos seguintes testes

- a. Teste de Conectividade TCP – Informando o Host e a Porta a serem testados;
- b. Teste de Conectividade ICMP – Informando o Host a ser testado;
- c. Teste de DNS – Informando o Host ou o Domínio a serem testados;
- d. Teste de Envio de E-mail ou Simular envio via porta 25 SMTP
- e. Teste de Conectividade com o fabricante (para isso, testa-se as portas e endereços necessários de comunicação junto ao fabricante, apresentando o resultado dessa comunicação ao administrador da solução);
- f. Teste de TRACEROUTE ou PING;
- g. Teste de DNS Reverso;
- h. Teste de SPF, para checar se tem registro para um determinado domínio;
- i. Teste de DKIM, para checar se tem registro para um domínio;
- j. Teste de DMARC, para checar se tem registro para um domínio;
- k. Teste de portas de Saída utilizadas pelo sistema;

4.12.13 Deve ter a capacidade de controle sobre os serviços executados no sistema, com a ação de: parar, inicializar ou reinicializar. O controle dos serviços devem ser sobre no mínimo os seguintes itens:

- a. Serviço de antivírus;
- b. Serviço de MTA;
- c. Serviço de Banco de Dados;
- d. Serviço de SNMP.

4.12.14. Características mínimas do MTA ofertado:

- 4.12.14.1. A solução contratada deverá possuir um software MTA focado em prover segurança, desempenho e alta disponibilidade;
- 4.12.14.2. O MTA deverá suportar filtros de conexões, que deverão ser executados antes que mensagens entrem no sistema, ou seja, antes do início do SMTP. Esses filtros deverão possuir a capacidade de classificar diferentes tipos de comportamento (como whitelist, blacklist, e gargalos). Os filtros de conexões deverão ser configuráveis, no mínimo, por:
- a) Endereço de IP;
 - b) Faixa de endereços de IP;
 - c) Deverão suportar RBL (listagem baseada em DNS);
 - d) Deverão possuir e utilizar filtros de reputação;
 - e) Deverão também possuir a capacidade de definição das políticas descritas nas letras abaixo:
 - f) Limite de número de destinatários por mensagem;
 - g) Limite do tamanho das mensagens;
 - h) Permitir a utilização ou não de SSL/TLS para conexão;
 - i) Utilização de antispam.
- 4.12.15. Deverá suportar SSL/TLS para conexões de entrada e saída;
- 4.12.16. Deverá ser capaz de utilizar DNS reverso nos conexões de entrada;
- 4.12.17. Deverá estar licenciado e ser capaz de processar o tráfego de mensagens para no mínimo 2000 caixas de e-mail;
- 4.12.18. Deverá suportar vários domínios (registros MX), e suportar roteamento de mensagens baseado em cada um desses domínios;
- 4.12.19. As filas de entrega do MTA deverão possuir tamanho suficiente para suportar uma sobrecarga de mensagens no evento de uma falha ou de um problema em outros pontos de infraestrutura de correio;
- 4.12.20. Deverá permitir o gerenciamento das filas de mensagens (queues), visualizando-as e com as opções de parar e iniciar as filas e de excluir (flush) mensagens;
- 4.12.21. Deverá suportar "aliasing";
- 4.12.22. Deverá suportar perfis únicos que tratam do comportamento de mensagens de volta (bounce) baseados nos domínios ou endereços IP de destino;
- 4.12.23. Deverá possuir "Message Tracking" na própria console gráfica para uma visualização detalhada do status da mensagem;
- 4.12.24. Deverá possibilitar a análise de URLs nos emails recebidos, protegendo assim os usuarios, contra URLs categorizadas como ameaça, que venham ser aberta pelo email;
- 4.12.25. Deverá suportar várias quarentenas residentes na própria solução, onde as mensagens deverão ser armazenadas pelo período de tempo especificado pelo administrador;
- 4.12.26. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena;
- 4.12.27. Deverá possuir a funcionalidade de dividir mensagens baseado em políticas definidas para cada: domínio, subdomínio, grupo de usuário, usuário individual, de forma integrada com ferramentas de LDAP,

AD, etc;

4.12.28. Deverá possibilitar a integração com múltiplos domínios de LDAP;

4.12.29. Deverá permitir a criação de políticas de antispam, filtros de conteúdo para cada um dos grupos criados;

4.12.30. Deverá permitir a criação de políticas, por usuários ou grupos, baseadas no tamanho ou tipo de anexo das mensagens;

4.12.31. Características mínimas dos filtros de reputação:

4.12.31.1. A solução contratada deverá possuir um sistema que permita estabelecer uma reputação (pontuação) dos endereços IP de servidores que estarão iniciando conexões TCP. Após estabelecida essa reputação, a solução deverá permitir ações diferenciadas de acordo com a pontuação obtida;

4.12.31.2. O sistema de verificação de reputação não deverá basear-se somente em RBL's públicas;

4.12.31.3. Esse sistema de reputação deverá utilizar uma conexão com base web nacional ou mundial, constantemente abastecida, por sua vez, de dados de várias fontes (black lists, outros appliance ou virtual appliances do mesmo fabricante implementados em outras organizações, etc.) – essa característica objetiva aumentar a precisão da pontuação fornecida;

4.12.31.4. O administrador deverá ter a possibilidade de aplicar políticas através dessa pontuação, podendo no mínimo, varrer por spam ou definir um tipo de proteção contra ameaças.

4.12.32. Características mínimas do software antispam:

4.12.32.1. Deverá possuir um sistema de regras que será atualizado automaticamente, numa frequência configurada pelo administrador;

4.12.32.2. Deverá possuir a possibilidade de ser configurada para analisar mensagens na entrada e na saída;

4.12.32.3. Filtrar mensagens baseadas na reputação das URLs inseridas em seu conteúdo;

4.12.32.4. Atualização automática dos filtros sem interrupção dos serviços e/ou perda das regras pré-estabelecidas pelo administrador;

4.12.32.5. Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

4.12.32.6. Ter a possibilidade de fazer approved list para domínios em se habilitando o domain keys identified mail (DKIM);

4.12.32.7. Possuir a detecção de SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta;

4.12.32.8. Permitir a criação de White e Black Lists para um melhor ajuste na detecção de SPAMs;

4.12.32.9. Permitir a proteção contra phishings;

4.12.32.10. Permitir verificar a reputação de links que estejam dentro do corpo das mensagens;

4.12.32.11. Possibilidade de White List para a checagem de reputação em URLs dentro de mensagens;

4.12.32.12. Possibilidade de se verificar o hash das mensagens em tempo real para proteção contra SPAMs.

4.12.33. Aspectos de segurança da solução:

- 4.12.33.1. Proteção contra Coleta do Diretório: a solução deverá possuir uma proteção contra esse tipo de ataque através da verificação integrada com LDAP, AD dos destinatários de mensagens;
- 4.12.33.2. Defesa contra ataque de Negação de Serviço: o solução deverá possuir a capacidade de identificar e proteger o MTA contra ataques por DoS;
- 4.12.33.3. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real;
- 4.12.33.4. Suportar o protocolo SMTP para análise de ameaças avançadas;
- 4.12.33.5 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF. Este deve utilizar técnicas de inspeção em tempo real baseadas em memória bloqueando até o veredito com múltiplos engines;
- 4.12.33.6. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;
- 4.12.33.7. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos emails com arquivos livres de malware;
- 4.12.33.8. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;
- 4.12.33.9. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;
- 4.12.33.10. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos;
- 4.12.33.11. Conter ameaças avançadas de dia zero;
- 4.12.33.12. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
- 4.12.33.13. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
- 4.12.33.14. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
- 4.12.33.15. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
- 4.12.33.16. Implementar a análise de arquivos executáveis, DLLs, ZIP no ambiente controlado;
- 4.12.33.17. Conter ameaças de dia zero de forma transparente para o usuário final;
- 4.12.33.18. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;
- 4.12.33.19. Conter ameaças de dia zero via tráfego de email;
- 4.12.33.20. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
- 4.12.33.21. Conter ameaças de dia zero que possam burlar o sistema operacional emulado;
- 4.12.33.22. A solução deve permitir a criação de White list;
- 4.12.33.23. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
- 4.12.33.24. Deverá ser capaz de checar e analisar ameaças tecnológicas utilizando tecnologia para mitigar os ataques cibernéticos;
- 4.12.33.25. A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações/processos são utilizadas para causar/propagar a infecção, detectar comandos/ações não confiáveis utilizadas pelo Malware, bloquear URLs não confiáveis nos emails e prover Informações sobre o usuário infectado (seu endereço IP ou seu login de rede);
- 4.12.33.26. Possuir recurso de firewall de email, protegendo o servidor de correio contra ataques de diretório (Directory Harvest Attack);

- 4.12.33.27. Possuir recurso de firewall de email ou blacklist, capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual ou uma quantidade de mensagens consideradas como SPAM, em um determinado espaço de tempo, ambos configuráveis pelo administrador;
- 4.12.33.28. A solução deverá permitir configuração de SSL/TLS;
- 4.12.33.29. A solução deverá funcionar de forma integrada ao Active Directory da Microsoft;
- 4.12.33.30. O sistema operacional e demais componentes da solução deverão possuir suporte ativo para recebimento de atualizações de segurança.
- 4.12.33.31. O sistema deve identificar e bloquear ataques que exploram vulnerabilidades na decodificação de domínios;
- 4.12.33.32. Prover mecanismo nativo para detecção, prevenção e bloqueio de diversos ataques sobre vulnerabilidade do protocolo SMTP, entre eles no mínimo:
 - a. SMTP Smuggling - CVE-2023-51764;
- 4.12.33.33. Deve prover um mecanismo que impeça a sua utilização como retransmissor de mensagens originadas externamente (relay);
- 4.12.33.34. Deve permitir a criação de regras baseadas por país;
- 4.12.33.35. Se a solução ofertada for do tipo SaaS (software como serviço), por questão de desempenho, garantia de sigilidade das informações e atendimento ao LGPD (Lei Geral de Proteção de Dados), através da instrução normativa nº5 de 30 de agosto de 2021 da legislação brasileira, um dos nodes da solução deve estar localizado no Brasil, para possível auditoria;
- 4.12.33.36. Se a solução ofertada for do tipo SaaS (software como serviço), utilizando a estrutura do fabricante, para garantia da idoneidade de uso do Datacenter e auditoria constante, o mesmo deve possuir certificação ISAE 3402 e ISO 27001;
- 4.12.33.37. Se a solução ofertada for do tipo SaaS (software como serviço), o sistema deverá manter os registros (logs) por pelo menos 6 meses, atendendo o Marco Civil da Internet no Brasil, sendo acessível ao administrador na própria console de gerenciamento (no modo gráfico, sem uso de linha de comando), sem necessidade de solicitar ao fabricante a liberação desses logs;

4.12.34. Filtros de Conteúdo contra spam deverão varrer todas as partes das mensagens, inclusive:

- 4.12.34.1. Emissores (comando SMTP MAIL FROM);
- 4.12.34.2. Destinatários (comando SMTP RCPT TO);
- 4.12.34.3. Cabeçalho do e-mail;
- 4.12.34.4. Corpo do e-mail;
- 4.12.34.5. Anexo(s) do e-mail.

4.12.35. O sistema de filtros deverá suportar dicionários de palavras e expressões regulares;

4.12.36. O sistema de anexos deverá possuir no mínimo:

- 4.12.36.1. Escaneamento por tipo MIME;
- 4.12.36.2. Escaneamento por anexos compactados;

4.12.37. Políticas baseadas na varredura deverão incluir pelo menos:

- 4.12.37.1. Entrega da mensagem;
- 4.12.37.2. Retorno da mensagem (bounce);
- 4.12.37.3. Descarte da mensagem;
- 4.12.37.4. Manipulação de cabeçalhos da mensagem;
- 4.12.37.5. Envio de mensagem de notificação para um outro endereço;
- 4.12.37.6. Envio de mensagem para quarentena.

4.12.38. As políticas deverão possuir capacidade de ser aplicadas usando as diretivas de grupo do Active Directory;

4.12.39. Os filtros de conteúdo deverão possuir capacidade de ser configurados para mensagens de e-mail na entrada e na saída;

4.12.40. O sistema deverá possuir capacidade para efetuar varredura de busca em outros idiomas ou byte duplo (UTF, por exemplo) para a busca em vários idiomas;

4.12.41. A solução deverá fornecer atualizações através de interface web e permitir prazo máximo de espera automática para realização de atualização.

4.12.42 A solução deverá fornecer os seguintes relatórios:

- 4.12.42.1. Sumário de mensagens;
- 4.12.42.2. Principais remetentes, por domínio ou por endereço de email;
- 4.12.42.3. Principais remetentes de SPAM, por domínio ou por endereço de email;
- 4.12.42.4. Principais destinatários de SPAM, por domínio ou por endereço de email;
- 4.12.42.5. Estatísticas sobre a quarentena ou notificações de quarentena;
- 4.12.42.6. Principais fontes de ataques de diretório ou relacionar os eventos das conexões bloqueadas;
- 4.12.42.7. Principais fontes de ataques de spam;
- 4.12.42.8. Volume de mensagens entre fontes e destinos ou permitir relacionar os maiores remetentes e destinatários;

4.12.43 Sobre os relatórios:

- 4.12.43.1 A solução deverá Possibilitar o agendamento e envio dos relatórios por email;
- 4.12.43.2 Os relatórios deverão suportar pelo menos os formatos HTML, CSV ou PDF.

4.12.44 A solução deverá fornecer uma interface gráfica com volumes em tempo real.

4.12.45 Recursos adicionais parametrizáveis da Solução:

4.12.45.1. Horário:

- 4.12.45.1.1. Permitir configuração de fuso horário;
- 4.12.45.1.2. Suportar configuração manual de horário;
- 4.12.45.1.3. Sincronizar via Network Time Protocol (NTP).

4.12.45.2. Alertas do sistema:

- 4.12.45.2.1. Possuir um sistema de alertas configurável pelo administrador;
- 4.12.45.2.2. Fornecer, pelo menos, avisos sobre eventos críticos no sistema, erros e notificações de alertas e possíveis ataques quarentenados;

4.12.45.3. Possuir suporte para integração de SNMP (Simple Network Management Protocol);

4.12.45.4. Integração com Serviço de Diretório:

- 4.12.45.4.1. Deverá integrar com vários fornecedores de serviços de diretório, dentre eles: LDAP (Lightweight Directory Access Protocol), AD (MS Active Directory);
- 4.12.45.4.2. Deverá integrar de forma anônima (sem senha) ou com usuário/senha para o envio e o recebimento de mensagens com suporte SSL/TLS.

4.12.45.5. Logs:

- 4.12.45.5.1. Possuir logs com um alto nível de detalhes ou possibilitar informações como (endereços IP e e-mail de origem e destino, reputação da origem, ou data, hora e políticas aplicadas);
- 4.12.45.5.2. Disponibilizados para acesso externo (FTP ou outro método);
- 4.12.45.5.3. Suportar modelo de envio (enviar logs para um servidor em horário pré-definido) e recebimento (um servidor de aplicação pode obter os logs) dos seus arquivos de “log”;

4.12.45.6 Filtros de Segurança:

- 4.12.45.6.1. Possuir mecanismos para identificação no conteúdo das mensagens de itens como: número de cartão de crédito, RG e/ou CPF, ou usar técnicas avançadas de machine learning e inteligência artificial para detectar malwares que simulam anexos, como CPF e outros documentos;
- 4.12.45.6.2. Possuir mecanismos para criação de diretórios de palavras pertencentes a temas específicos como, por exemplo, ofensas, ou tecnologias que possibilitem uma análise profunda, permitindo a criação de filtros e regras voltadas à proteção contra tentativas de evasão de dados. ;
- 4.12.45.6.3. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;
- 4.12.45.6.4. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;
- 4.12.45.6.5. Permitir que arquivos suspeitos sejam enviados ao fabricante sem intervenção do administrador;
- 4.12.45.6.6. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;
- 4.12.45.6.7. Proteção contra Spywares, sem a necessidade de um software ou agente adicional;
- 4.12.45.6.8. Proteção contra Ferramentas Hackers, sem a necessidade de um software ou agente adicional;

- 4.12.45.6.9. Proteção contra Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;
- 4.12.45.6.10. Proteção contra Adwares, sem a necessidade de um software ou agente adicional;
- 4.12.45.6.11. Bloqueio de malware empacotado (packed malware) de forma heurística.

4.12.45.7. Administração via console de gerenciamento:

- 4.12.45.7.1. Atualizar automaticamente os filtros, sem interrupção dos serviços;
- 4.12.45.7.2. Possuir console de administração interna ao produto, Web, sem necessidade de instalar clientes ou partes da solução em máquinas adicionais para a administração;
- 4.12.45.7.3. Gerenciamento via console web HTTPS (Internet Explorer / Google Chrome / Firefox).

4.12.45.8. A solução deve possuir um passo a passo de instalação e configuração;

4.12.45.9. Realizar atualização de forma automática das vacinas de forma incremental. A atualização deve permitir conexão através de serviço Proxy;

4.12.45.10. Possuir autenticação via TLS (Transport Layer Security);

4.12.45.11. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

4.12.45.12. A interface de administração deverá possuir acesso criptografado (HTTPS ou através de software de gerenciamento, do mesmo fabricante da Solução, com diversos níveis de privilégio. Os tipos mínimos serão “administração”, “relatórios”, “quarentena” e “apenas leitura”;

4.12.45.13. Possuir quarentena por usuário proprietária do mesmo fabricante desenvolvedor da tecnologia de anti-spam fornecida, possibilitando ao usuário administrar sua própria quarentena, removendo mensagens ou liberando as que não considera SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos. A Quarentena pode ser implementada com integração direta em aplicações de correio eletrônico, ou via interface Web (HTTPS);

4.12.45.14. Capacidade de apresentar uma console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;

4.12.45.15. Capacidade de usuários criarem lista de exceções a remetentes nessa console web de quarentena de mensagens;

4.12.45.16. Permitir que os usuários verifiquem mensagens suspeitas postas em quarentena e aprovar os remetentes sem intervenção do administrador;

4.12.45.17. Permitir exclusão automática das mensagens em quarentena;

4.12.45.18. Permitir que o próprio usuário crie listas brancas (de endereços confiáveis) pessoais, independente do administrador, e de forma que estas listas brancas não interfiram nos filtros de outros usuários;

4.12.45.19. O módulo de quarentena deverá residir no próprio sistema do antispam e ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena;

4.12.45.20. Deve efetuar remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

4.12.45.21. Possuir funcionalidade de criação de “alias” ou mascaramento de endereço;

4.12.46 Requisitos para solução baseada em Appliance Físico:

4.12.46.1 Deve ser com hardware do próprio fabricante ou hardware homologado pelo fabricante para execução do software;

4.12.46.2. Cada appliance deve permitir montagem em rack com largura padrão de 19 polegadas;

4.12.46.3. Cada appliance deve possuir dimensão não superior a 2U's;

4.12.46.4. As faixas de tensão de entrada suportadas por cada appliance devem ser de 100V (corrente alternada) a 127V (corrente alternada) e de 200V (corrente alternada) a 240V (corrente alternada), a 6

0Hz, sem uso de chave de seleção de voltagem (voltagem automática), capaz de sustentarem a configuração máxima do equipamento;

4.12.46.5 A solução deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

4.12.46.6 Cada appliance deve possuir quantidade de memória e poder de processamento suficientes para atendimento de todas as funcionalidades e desempenhos solicitados neste documento;

4.12.46.7 O sistema operacional deve estar embutido no hardware proposto, ou seja, hardware e software devem ser integrados em um único equipamento;

4.12.46.8 Não serão aceitos componentes da solução ofertada usados, remanufaturados ou de demonstração;

4.12.46.9 Na data da proposta, o equipamento ofertado não poderá estar listado no site do fabricante em listas de end-of-life e end-of-sale;

4.13. Instalação e Configuração - Item 02 :

4.13.1. A licitante vencedora deverá disponibilizar, no prazo constante deste Termo de Referência, técnicos devidamente certificados junto ao fabricante da solução ofertada para realizar todos os serviços de instalação;

4.13.2. Os técnicos designados para essa missão deverão possuir experiências no processo de implantação de solução de filtragem de e-mails;

4.13.3. Todos os serviços serão assistidos pela equipe da Seção de Segurança Cibernética ou pela Seção de Redes do Tribunal, as quais darão todo apoio e condições necessárias para realização das atividades;

4.13.4. O serviço de instalação somente será aceito quando todas as funcionalidades estipuladas neste Termo de Referência estiverem com status operacional;

4.13.5. O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias corridos após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada.

4.13.16. O recebimento definitivo dos serviços de instalação e migração se dará no prazo de 10 (dez) dias corridos após o recebimento provisório e se for constatada a estabilidade operacional da solução implantada.

4.13.17. No caso de appliance físico a instalação deverá ser feita presencialmente no Prédio Sede do TRE-PB (Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58013-251 - João Pessoa - PB) e/ou no Fórum Eleitoral de João Pessoa-PB (R. Dep. Odon Bezerra, 309 - Bairro - Tambiá - CEP 58020-500 - João Pessoa - PB).

4.14. Repasse Tecnológico - Item 03 :

4.14.1. A contratada deverá ministrar treinamento, na língua portuguesa, para até 10 (dez) servidores indicados pelo órgão, com carga horária mínima de 20 horas.

4.14.2. O conteúdo do treinamento a ser ministrado deverá contemplar os seguintes itens:

- a. Procedimentos de instalação;
- b. Todos os procedimentos necessários à configuração técnica;
- c. Todos os procedimentos necessários à completa operação do produto;
- d. Todos os procedimentos de manutenção do produto que devem ser realizados pelos técnicos do órgão.

4.14.3. O treinamento poderá ser realizado virtualmente por profissional certificado pelo fabricante do produto ofertado;

4.14.4. O treinamento deverá ser ministrado em horário definido pelo tribunal, em dias úteis;

4.14.5. O treinamento será dado como concluído após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento, com a reformulação que achar necessária.

4.14.6. O Repasse Tecnológico deverá ser feito por técnicos devidamente certificados junto ao fabricante da solução ofertada.

4.15. Suporte Técnico Especializado - Item 04 :

4.15.1. A Contratada deverá fornecer os serviços de suporte, durante o período coberto pela garantia da solução de filtragem de e-mails, que será de 36 Meses, compreendendo, no mínimo as seguintes atividades:

- a) Acompanhar, quando solicitado pela CONTRATANTE, todas as operações realizadas no sistema durante determinado período de tempo, sempre que constatada a necessidade pela contratada e notificado a contratante através da Web, E-mail ou telefone;
- b) Esclarecer dúvidas de usuários em relação à operação do sistema e/ou solução ofertada;
- c) Prestar serviços de suporte técnico para a solução na modalidade de 24x7 (24 horas/dia e 7 dias/semana);
- d) Reportar à CONTRATANTE quaisquer outros problemas verificados durante o atendimento, relativos ou não à solução ofertada;
- e) Fornecer informações aos usuários da CONTRATANTE sobre a situação e o andamento de serviços de manutenção e/ou consultivos solicitados;
- f) Diagnosticar a performance do solução em seus aspectos operacionais;
- g) Identificar e notificar problemas inerentes ao software e/ou solução;
- h) Notificar possíveis problemas de performance oriundos do ambiente onde a solução se encontra instalada;
- i) Discutir implementações de melhorias e atualizações, visando possíveis adequações;
- j) Na prestação dos serviços, quando solicitado pela CONTRATANTE, a CONTRATADA utilizará profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas;
- k) Apoiar na criação de dashboards e relatórios da software e/ou solução;
- l) Apoiar na solução de problemas relativos a solução e às licenças adquiridas para chamados Nível 1 (padrão);

m) Intermediação, acompanhamento e suporte entre a CONTRATANTE e o fabricante da solução para chamados Nível 2, 3 e 4;

4.15.2. O Fornecimento desse requisitos integrantes da Solução de Filtragem de e-mails implicará na prestação continuada coberta pela garantia do fabricante, atualizações de firmware, ativação completa para todas as funcionalidades de segurança descrita neste Termo de Referência, incluindo atualização dinâmica das proteções aqui elencadas e demais recursos de segurança que requeiram atualização frequente;

4.15.3. As atualizações e upgrades de software e firmware devem ser disponibilizadas à CONTRATANTE para download no site da CONTRATADA ou do fabricante.

4.15.4. O serviço de suporte técnico pelo período de Garantia contratado deverá ser prestado através do acionamento da CONTRATADA, para atendimento das necessidades de informação e restabelecimento de funcionalidades nas condições e prazos a seguir:

4.15.4.1. Para correção de funcionalidade impactada e que não impede a continuidade da maior parte dos negócios, será considerada como de **SEVERIDADE BAIXA: Prazo máximo para resolução: 48 horas**;

4.15.4.2. Para solicitação de informações sobre os produtos, incluindo configuração e instalação, será considerada de **SEVERIDADE BAIXA: Prazo máximo para resolução: 36 horas**;

4.15.4.3. Para problemas que causem impactos significativos nos negócios incluindo degradação de desempenho, serão considerados como de **SEVERIDADE MÉDIA: Prazo máximo para resolução: 24 horas**;

4.15.4.4. Para situações em que os serviços se encontrem indisponíveis, serão consideradas como de **SEVERIDADE ALTA: Prazo máximo para resolução será de 8 horas**. Havendo necessidade de substituição de equipamentos o prazo de resolução do problema será no máximo de 24 horas.

4.15.5. A manutenção em garantia poderá ser realizada pelo fabricante, porém, sendo responsabilidade subsidiária da CONTRATADA;

4.15.6. A CONTRATADA deverá enviar o documento comprobatório da ativação dos Requisitos de Segurança integrantes da Solução de filtragem de E-mails à Seção de Segurança Cibernética (SESEC), através dos e-mails sesec@tre-pb.jus.br, confirmando através do telefone: (83) 3512-1420.

4.15.7. A CONTRATADA deverá aceitar as especificações de softwares e protocolos de segurança estabelecidos pela CONTRATANTE para a realização do acesso remoto.

4.15.8. O Suporte Técnico Especializado deverá ser feito por técnicos devidamente certificados junto ao fabricante da solução ofertada.

4.16 - Garantia técnica dos serviços

A Contratada deverá prestar garantia técnica dos serviços executados e dos produtos entregues durante toda a vigência do contrato, incluindo suas prorrogações.

A garantia técnica deverá corrigir todos e quaisquer defeitos nos produtos entregues ou nos serviços prestados pela Contratada que compreendem, dentre outros: os erros e falhas de configuração, instalação, operação, causados por ações ou omissões da Contratada; as imperfeições percebidas e qualquer outra ocorrência que impeça o funcionamento normal dos serviços contratados ou que não se apresente dentro dos padrões e níveis de qualidade predefinidos por este Termo de Referência, mesmo após o aceite definitivo por parte do Contratante.

As documentações vinculadas às entregas de serviços também estarão cobertas pela garantia técnica.

A Contratada deverá garantir a qualidade técnica de cada serviço ou produto fornecido por ela, estando obrigada a reparar e melhorar aquele que apresentar inconsistência total ou parcial no decorrer de sua utilização durante a vigência contratual.

Os serviços em garantia técnica executados pela Contratada em atividades total ou parcialmente rejeitadas, não afastam a aplicação de penalidades e de outras sanções previstas no contrato, conforme o caso.

Durante a execução da garantia técnica, todas as despesas com a equipe para o atendimento de garantia serão custeadas pela Contratada, sem ônus para o Contratante.

4.17 - Garantia da contratação

4.15.1 A Contratada deverá prestar garantia contratual no percentual de 2% (dois por cento), do valor total do contrato, nos termos do artigo 96 da Lei nº 14.133/2021, com validade durante a execução do contrato e até 90 (noventa) dias após o término da sua vigência, devendo ser renovada a cada prorrogação.

4.15.2 Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.15.3 A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

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

4.18 - Requisitos de cumprimento da Lei Geral de Proteção de Dados - Lei Nº 13.709/2018

4.18.1 A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE.

4.18.2 Em atendimento ao disposto na Lei Geral de Proteção de Dados, o CONTRATANTE, para a execução do serviço objeto deste contrato, tem acesso a dados pessoais dos representantes da CONTRATADA, tais como números do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação.

4.18.3 As partes obrigam-se a cumprir o disposto na Lei nº 13.709/2018 em relação aos dados pessoais a que venham ter acesso em decorrência da execução contratual, comprometendo-se a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassadas em decorrência da execução contratual, sendo vedada a transferência, a transmissão, a comunicação ou qualquer outra forma de repasse das informações a terceiros, salvo as decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

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

4.18.5 A Contratada fica obrigada a comunicar ao Contratante, em até 24 (vinte e quatro) horas, a contar da ciência do ocorrido, qualquer incidente de segurança aos dados pessoais repassados em decorrência desta contratação e a adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados Pessoais.

4.18.6 As partes responderão administrativa e judicialmente na hipótese de causarem danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

4.18.7 As partes obrigam-se a proceder, ao término do prazo de vigência, à eliminação dos dados pessoais a que venham ter acesso em decorrência da execução contratual, ressalvados os casos em que a manutenção dos dados por período superior decorra de obrigação legal.

5. Modelo de gestão do contrato, que descreve como a execução do objeto será acompanhada e fiscalizada pelo TRE/PB (Art. 6º, XXIII, "f", da Lei nº 14.133/2021):

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

6.2 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.

6.3 Após a assinatura do contrato e a nomeação do gestor e fiscais do contrato, será realizada a reunião inicial de alinhamento com o objetivo de nivelar o entendimento acerca das condições estabelecidas no contrato, edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

6.4 A execução do contrato deverá ser acompanhada e fiscalizada pelos fiscais do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da Instrução Normativa nº 94/2022-SGD/ME.

6.5 O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da Instrução Normativa nº 94/2022-SGD/ME, acompanhará a execução do contrato, para que sejam cumpridas todas as condições nele estabelecidas, de modo a assegurar os melhores resultados para a Administração. Ademais, ele anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Decreto nº 11.246/2022, art. 22, II](#)).

6.6 Identificada qualquer inexatidão ou irregularidade, o fiscal técnico emitirá notificação para a correção da execução do contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#));

6.7 O fiscal técnico do contrato informará ao gestor do contrato, 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](#)).

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

6.9 O fiscal técnico do contrato comunicará 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](#)).

6.10 O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da Instrução Normativa nº 94/2022-SGD/ME, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da solicitação de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. ([Decreto nº 11.246, de 2022, art. 21, IV](#)).

6.11 O gestor do contrato verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

6.12 Caso ocorra descumprimento das obrigações contratuais, o gestor atuará tempestivamente na solução do problema.

6.13 O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, 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](#)).

6.14 O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico e administrativo quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. ([Decreto nº 11.246, de 2022, art. 21, VIII](#)).

6.15 O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções ([Decreto nº 11.246, de 2022, art. 21, X](#)).

6.16 O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

6.17 O gestor do contrato deverá enviar a documentação pertinente à Coordenadoria de Serviços Gerais para a formalização dos procedimentos de liquidação e pagamento no valor dimensionado pela fiscalização e gestão nos termos do contrato.

6.18 Quanto às sanções e ao procedimento a ser adotado, serão aplicadas as previstas na Lei nº 14.133/2021 e no normativo interno deste Regional pertinente ao assunto, bem com o contrato regulará melhor a matéria.

6. Do pagamento :

6.1. O pagamento será feito em duas etapas:

6.1.1 O valor da primeira etapa será o somatório dos valores dos itens 1,2 e 4 e será pago após a entrega dos itens 1 e 2;

6.1.2 O valor da segunda etapa será o valor do item 3 e será pago após a entrega do item 3.

6.1.3 Da justificativa para pagamento O pagamento em parcela única dos itens 1 e 4, se justifica pelos seguintes motivos:

6.1.3.1. REDUÇÃO DE CUSTOS

6.1.3.1.1. O pagamento em parcela única geralmente resulta em custos totais menores em comparação com o pagamento mensal. Isso ocorre porque as empresas licitantes podem obter descontos significativos com os fabricantes, uma vez que não precisam se preocupar com a administração de pagamentos mensais e os riscos associados à cobrança, como atraso nos pagamentos e possível incidência de juros às licitantes, reduzindo a margem de lucro das mesmas, o que corrobora com a redução do preço final para a CONTRATANTE;

6.1.3.1.2. A não incidência de juros do financiamento da solução junto aos fabricantes das ferramentas

(hardware e licenciamento/subscrição), ou mesmo junto aos bancos, que estaria embutido no preço mensal e final estimado da solução ofertada, é menor, ou até mesmo não existe quando há previsão de pagamento em parcela única, o que impacta sobre maneira na redução dos custos e valores finais estimados para a CONTRATANTE;

6.1.3.1.3. A variação dos preços dos componentes da solução ofertada que são baseadas em moeda Americana (\$US – Dolar), também reduz os custos totais de contratos com pagamento em parcela única, frente aos contratos com pagamento parcelado mensal, pois sobre estes pode incidir variação, aumento no valor da moeda Americana, o que resultaria em um custo maior, e conseqüentemente um risco maior, o que impactaria no repasse desse custo ao valor do pagamento mensal e no valor final da solução, ao final do período de vigência contratual, e não havendo esta variação no valor da moeda Americana, não há repasse desse valor na estimativa de custos para a CONTRATANTE;

6.1.3.1.4. Todos os itens acima corroboram com a redução do preço final para a CONTRATANTE.

6.1.3.2. AGILIDADE NA IMPLEMENTAÇÃO

6.1.3.2.1. Em função do pagamento em parcela única, a empresa CONTRATADA poderá acelerar a implementação da solução, a mesma pode ocorrer de forma mais rápida e eficiente, o que beneficiaria a CONTRATANTE, com a entrega da solução operacional em um prazo menor;

6.1.3.2.2. Ganho no resultado e na proteção do ambiente com a implementação da solução de forma mais célere, antes do tempo previsto em contrato, resultando na redução de riscos relacionados e aproveitamento mais rápido dos benefícios advindos da solução contratada pela CONTRATANTE

6.1.3.3. REDUÇÃO NO ÔNUS ADMINISTRATIVO

6.1.3.3.1. O pagamento em parcela única reduz a burocracia e a complexidade administrativa mensal para gestão do contrato pela equipe da CONTRATANTE;

6.1.3.3.2. Não há necessidade de validação mensal de entregas, que em contratos com pagamento mensal são necessárias, e se descumpridas condicionam o pagamento e impõe a aplicação de glosas, situação que exige da equipe de gestão do contrato grande esforço.

6.1.3.3.3. Em contrapartida, em contratos com pagamento em parcela única, o ônus administrativo para equipe de gestão do contrato, é mínima, normalmente quando há necessidade de acionar o serviço de garantia e suporte previstos em contrato.

6.1.3.4. O princípio da economicidade é um dos princípios fundamentais que norteiam a administração pública. Ele estabelece que a gestão dos recursos públicos deve ser realizada de forma eficiente e econômica, visando à obtenção dos melhores resultados possíveis

com o menor custo possível, e o pagamento em parcela única, frente ao pagamento mensal, demonstra a aplicação efetiva deste princípio.

6.1.3.5. A escolha pelo modelo de pagamento em parcela única aumenta muito o poder de negociação das licitantes junto aos fabricantes, afinal, a previsão de recebimento de forma única, concede a possibilidade de solicitar descontos mais agressivos e negociações com reduções

maiores dos preços, o que resulta em uma oferta mais vantajosa para a Administração, para a CONTRATANTE.

6.1.3.6. Corroborando ainda com o a adoção de pagamento em parcela única o fato de que para soluções de Tecnologia da Informação esse modelo é uma praxe do mercado, e como exemplo podemos citar contratações de soluções de Microsoft, como o pacote Microsoft 365, oferecido pelos parceiros da mesma, que são normalmente pagos em parcela única. Outros exemplos seriam as contratações conjuntas realizadas em 2022 e 2023 pelos Tribunais Regionais Eleitorais, todas também foram realizadas dessa forma.

6.1.3.7. Conclui-se assim, que a adoção do modelo de pagamento parcela única é administrativa e economicamente mais vantajosa para a CONTRATANTE.

Recebimento

6.2. Os serviços serão recebidos, de forma provisória, de acordo com as entregas e etapas do item 6.1, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

6.2.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a etapa a a ser paga.

6.3. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo que comprove o cumprimento das exigências deste Termo de Referência. (Art. 22, X, Decreto nº 11.246, de 2022).

6.4. Para efeito de recebimento provisório, ao final de cada etapa de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados.

6.4.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo de recebimento provisório;

6.5. O Contratado fica obrigado 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 ou materiais empregados, cabendo à fiscalização não atestar a prestação de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

6.6. 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)

6.7. 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.

6.8. Os serviços serão recebidos definitivamente no prazo de 05 (dias) 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, obedecendo os seguintes procedimentos:

6.8.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

6.8.2. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

6.8.3. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

6.8.4. Enviar a documentação pertinente a Secretária de Administração e Orçamento para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

6.9. 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.

6.10. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.11. 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.

Liquidação

6.12. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º, da Instrução Normativa SEGES/ME nº 77/2022.

6.12.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133/2021, por força do disposto no art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

6.13. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão CONTRATANTE;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar e
- f) eventual destaque do valor de retenções tributárias cabíveis.

6.13. 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.

6.14. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à

documentação mencionada no art. 68 da Lei nº 14.133/2021.

6.15. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do TRE-PB, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

6.16. Constatando-se, junto ao SICAF, a 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 da CONTRATANTE.

6.17. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

6.18. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

6.19. 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.

Prazo de pagamento

6.20. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da [Instrução Normativa SEGES/ME nº 77/2022](#).

6.20.1 O prazo de que trata o item anterior será reduzido à metade, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133/2021, por força do disposto no art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

6.21. Havendo atraso no pagamento de suas obrigações, o TRE/PB procederá à atualização financeira diária de seus débitos, onde os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, conforme a seguinte fórmula:

$$I = (TX / 100) \cdot 365$$

$$EM = I \times N \times VP$$

onde: I = Índice de atualização financeira; TX = Percentual da taxa de juros de mora anual; 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.

Forma de pagamento

6.22. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

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

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

6.25. 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.

6.26. 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 Lei Complementar.

7. Papéis e responsabilidades:

7.1. São obrigações da Contratante:

- a. Receber provisoriamente o material, disponibilizando local, data e horário.
- b. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos.
- c. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através do gestor e dos fiscais especialmente designados.
- d. Efetuar o pagamento na forma e no prazo previsto neste instrumento e no contrato.

7.2. São obrigações da Contratada:

Além das demais obrigações descritas ao longo deste Termo de Referência, a CONTRATADA obriga-se a:

- a. Fornecer todas as licenças de software necessárias para utilização completa da solução pelos períodos adquiridos, salvo o sistema operacional das máquinas utilizadas pela solução.
- b. Registrar, junto aos fabricantes e em nome da contratante, todas as assinaturas de licenças de software ofertadas.
- c. Cumprir fielmente as obrigações assumidas, conforme as especificações constante neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos/prestar os serviços, nos prazos indicados.

- d. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da entrega dos objetos licitados no local indicado, incluindo os possíveis danos causados por transportadoras, sem qualquer ônus ao contratante.
- e. Prestar todos os esclarecimentos que forem solicitados pelo TRE-PB, credenciando junto ao órgão, um representante para prestar os devidos esclarecimentos e atender as reclamações que porventura surgirem durante a execução do objeto.
- f. Assinar, através de seu responsável legal, Termo de Sigilo e Responsabilidade, garantindo o sigilo e a confidencialidade dos dados a que vier a ter contato durante a instalação e durante a utilização da solução de software.
- g. A contratada obrigar-se-á em manter-se em compatibilidade com a habilitação e com as obrigações assumidas na licitação até o adimplemento total da contratação.
- h. Executar os serviços nos prazos estabelecidos neste instrumento, nos locais indicados pela Administração, em estrita observância das especificações do Edital e da proposta
- i. Atender prontamente aos chamados da Administração, relacionados ao objeto da licitação.
- j. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
- k. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- l. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.
- m. Apresentar junto com a Fatura/Nota Fiscal dos serviços prestados, as comprovações de regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF) e às Fazendas Federal, Estadual e Municipal de seu domicílio ou sede, bem como a Certidão Negativa de Débitos Trabalhistas de que trata a Lei nº 12.440/2011; caso esses documentos não estejam disponíveis no SICAF.
- n. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nos casos e condições autorizadas pelo CONTRATANTE, já previstos neste Termo de Referência.

8. Forma e critérios de seleção do fornecedor (Art. 6º, XXIII, "h", da Lei nº 14.133/2021):

8.1. Forma de seleção e critério de julgamento da proposta:

8.1.1. Considerando a natureza comum do objeto da contratação pretendida, conforme exposto nos estudos técnicos preliminares, o fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade pregão, sob a forma eletrônica, de acordo com o artigo 29, da Lei nº 14.133/2021.

8.1.2. O critério de julgamento a ser utilizado será o menor preço, com esteio no artigo 33,

I, da Lei nº 14.133/2021.

8.2. Aplicação de margem de preferência:

8.2.1 Não se aplica o [Decreto nº 7.174/2010](#).

8.3. Habilitação jurídica:

8.3.1 As exigências de habilitação jurídica e de regularidade fiscal, social e trabalhista são as disciplinadas no edital.

8.4. Qualificação econômico-financeira:

8.4.1 Considerando a importância do objeto desta contratação para a área de segurança da informação do correio eletrônico e o seu impacto nas atividades meio e fim deste Regional, é de grande relevância que a empresa licitante detenha esteio financeiro suficiente para suportar a contratação pretendida, com fito de realizar a sua devida execução.

8.4.2 Assim, a qualificação econômico-financeira deve incluir os seguintes documentos:

- Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - [Lei nº 14.133, de 2021, art. 69, caput, inciso II](#));
- Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:
 - I - Liquidez Geral (LG) = $(\text{Ativo Circulante} + \text{Realizável a Longo Prazo}) / (\text{Passivo Circulante} + \text{Passivo Não Circulante})$;
 - II - Solvência Geral (SG) = $(\text{Ativo Total}) / (\text{Passivo Circulante} + \text{Passivo não Circulante})$; e
 - III - Liquidez Corrente (LC) = $(\text{Ativo Circulante}) / (\text{Passivo Circulante})$.
- Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% do

valor total estimado da contratação.

- As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (art. 65, §1º, da Lei nº 14.133/2021).
- O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (art. 69, §6º, da Lei nº 14.133/2021).
- Comprovação, por meio de declaração, da relação de compromissos assumidos de que 1/12 (um doze avos) do valor total dos contratos firmados com a Administração Pública e/ou com a iniciativa privada, vigentes na data da sessão pública de abertura deste pregão, não é superior ao patrimônio líquido da licitante, podendo esse ser atualizado na forma disciplinada no edital. (art. 69, §3º, da Lei nº 14.133/2021).

8.5. Qualificação técnica-operacional:

8.5.1 As empresas interessadas na contratação deverão apresentar a seguinte documentação para fins de qualificação técnico-operacional:

8.5.2 Comprovação de aptidão para a prestação dos serviços em características, quantidades e volumes compatíveis com o objeto desta licitação, por período não inferior a 3 (três) anos, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado;

8.5.3 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

8.5.4 Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da [Instrução Normativa nº 05/2017 - SEGES/MPDG](#);

8.5.5 Para a comprovação da experiência mínima de 3 (três) anos, será aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os três anos serem ininterruptos, conforme item 10.7.1 do Anexo VII-A da [Instrução Normativa nº 05/2017 - SEGES/MPDG](#);

8.5.6 Em caso de dúvida na análise dos atestados em relação às exigências acima, poderá haver diligência nesse sentido.

8.5.7 A pregoeira poderá diligenciar acerca da veracidade das informações constantes nos atestados e nos documentos apresentados. Assim, poderão ser exigidos contratos, ajustes, solicitações de serviço, solicitações de pagamento, notas fiscais, termos de aceite, planilhas, relatórios, gráficos, documentação de sistemas e ambiente operacional, documentação de gestão de projetos, sistemas informatizados, base de dados, controle de versão e outros, a fim de sanar dúvidas decorrentes dos atestados apresentados. Caso seja constatada divergência entre as informações atestadas e os serviços efetivamente realizados, o atestado será desconsiderado. Caso fique caracterizada atitude inidônea da licitante, essa estará sujeita às penalidades previstas em lei.

8.5.8 O(s) atestado(s) deve(m) ser fornecido(s) por pessoa jurídica de direito público ou privado e conter nome (razão social), CNPJ e endereço completo do respectivo contratante e da contratada, características dos serviços realizados, data de emissão, nome, cargo, telefone e assinatura do responsável por sua emissão.

8.5.9 A exigência de atestado(s) com prazo não inferior a 3 (três) anos se justifica pela necessidade de assegurar o perfeito cumprimento do contrato por empresa idônea e com expertise suficiente para evitar prejuízos ao Erário.

8.6. Parcelamento ou não da solução:

8.6.1 O parcelamento não é considerado viável, pois ensejaria vários contratos, com fornecedores diferentes, para o mesmo serviço, aumentando o custo deste Regional com a gestão contratual. Assim, com base no artigo 47, §1º, II, da Lei nº 14.133/2021, opta-se pelo não parcelamento, com a concentração dos esforços da equipe responsável no acompanhamento de um único contrato, permitindo uma maior eficiência, uma vez que o número de servidores é muito reduzido.

9. Adequação orçamentária (Art. 6º, XXIII, "i", da Lei nº 14.133/2021):

9.1 A despesa decorrente deste contrato correrá à conta de recursos específicos consignados no orçamento da União.

9.2 A contratação será atendida pela seguinte dotação:

I- Gestão/Unidade: SESEC

II- Fonte de recursos: Recursos suplementares de cibersegurança oriundos de iniciativa do TSE (SEI 0001331-13.2024.6.15.8000)

10. INFRAÇÕES ADMINISTRATIVAS E SUAS SANÇÕES:

10.1. Comete infração administrativa, nos termos da [Lei nº 14.133, de 2021](#), o licitante ou o contratado

que:

- I - der causa à inexecução parcial do contrato;
- II - der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- III - der causa à inexecução total do contrato;
- IV - deixar de entregar a documentação exigida para o certame;
- V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação e
- XII - praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

10.2. O licitante ou o contratado que incorrer em infração administrativa prevista na alínea anterior, apurada em regular processo administrativo, com garantia de contraditório e ampla defesa, sujeitar-se-á às seguintes sanções:

- I - advertência;
- II - multa;
- III- impedimento de licitar e contratar;
- IV - declaração de inidoneidade para licitar ou contratar.

10.3. A aplicação das sanções previstas no item anterior não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

10.4. A sanção de advertência será aplicável na hipótese de inexecução parcial do contrato que não implique em grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo, bem como na hipótese de descumprimento de pequena relevância praticado pelo contratado e que não justifique imposição de penalidade mais grave.

10.5. A multa será aplicada, isolada ou cumulativamente com outras penalidades previstas no item 10.2, ao responsável por qualquer das infrações administrativas previstas no item 10.1.

10.6. A multa compensatória será calculada no percentual de 15% (quinze por cento) do valor da contratação.

10.7. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será obtida observando-se a seguinte ordem:

I - utilização da garantia eventualmente prestada;

II - compensação dos créditos de outros contratos firmados pela contratada com este Regional, na forma da [Instrução Normativa SEGES/ME nº 26/2022](#);

III - por via judicial.

10.8. O atraso injustificado na execução do pactuado sujeitará a contratada a multa de mora de 0,5% (zero vírgula cinco por cento) ao dia sobre do saldo da contratação, limitado a 15%.

10.9. A aplicação de multa moratória não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções dispostas no item 10.2.

10.10. A sanção de impedimento de licitar e contratar prevista no item 10.2 será aplicada ao responsável pelas infrações administrativas previstas nos [itens II, III, IV, V, VI e VII](#) do item 10.1, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta da União, pelo prazo máximo de 3 (três) anos.

10.11. A sanção de declaração de inidoneidade para licitar ou contratar será aplicada ao responsável pelas infrações administrativas previstas nos [itens VIII, IX, X, XI e XII](#) do item 10.1, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do referido item que justifiquem a imposição de penalidade mais grave que a sanção citada no 10.10, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

10.12. A aplicação das sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar requererá a condução de processo de responsabilização por Comissão Permanente de Responsabilização de Licitantes e Contratados - CPRLC.

10.13. Para a aplicação de qualquer sanção, deverá ser adotado o procedimento previsto neste instrumento, na [Portaria nº 301/2023 TRE-PB/PTRE/ASPRE](#) e na Lei nº 14.133/2021.

11. Integram este documento os seguintes anexos:

ANEXO I- Modelo de Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB (1873110)

ANEXO II – Modelo de Declaração de Ciência do Termo de Responsabilidade e Confidencialidade das Informações do TRE/PB (1873116)

12. Equipe de Fiscalização:

Gestor do contrato titular - Felipe Cavalcanti Alves

Gestor do contrato substituto - Pedro de Figueirêdo Lima Neto

Fiscal técnico titular - Airton Alves de Medeiros Junior

Fiscal técnico substituto - José Cassimiro Junior

FELIPE CAVALCANTI ALVES
CHEFE DA SEÇÃO DE SEGURANÇA CIBERNÉTICA



Documento assinado eletronicamente por FELIPE CAVALCANTI ALVES em 06/09/2024, às 18:01, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

PEDRO DE FIGUEIRÊDO LIMA NETO
CHEFE DA SEÇÃO DE INFRAESTRUTURA DE REDE



Documento assinado eletronicamente por PEDRO DE FIGUEIRÊDO LIMA NETO em 06/09/2024, às 18:22, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

FABIANA BIONE MAIA DE ALMEIDA FERREIRA POLARI
ANALISTA JUDICIÁRIO



Documento assinado eletronicamente por FABIANA BIONE MAIA DE ALMEIDA FERREIRA POLARI em 06/09/2024, às 18:48, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).

JOSÉ CASSIMIRO JUNIOR
COORDENADOR(A) DE ELEIÇÕES INFORMATIZADAS E SEGURANÇA CIBERNÉTICA



Documento assinado eletronicamente por JOSÉ CASSIMIRO JUNIOR em 09/09/2024, às 13:11, conforme art. 1º, III, "b", da [Lei 11.419/2006](#).



A autenticidade do documento pode ser conferida no site https://sei.tre-pb.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1904605&crc=8F9F2001, informando, caso não preenchido, o código verificador **1904605** e o código CRC **8F9F2001**.