



CONSELHO REGIONAL DE MEDICINA DO ESTADO DA PARAÍBA

TERMO DE REFERÊNCIA (TR)

João Pessoa, 01 de outubro de 2026

ANEXO I - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO

SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO-DE-OBRA

ÓRGÃO(S) REQUISITANTE (S): CONSELHO REGIONAL DE MEDICINA - CRM/PB

1. CONDIÇÕES GERAIS DE CONTRATAÇÃO

1.1. Contratação de serviços de Firewall com fornecimento de equipamentos de TI e suporte de equipamentos, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Grupo	Item	Código CATSER	Especificação	Unidade de Medida	Quantidade	Valor Mensal Total Estimado	Valor Anual Estimado (R\$)
Único	1	27502	Solução de Segurança Cibernética Distribuída NGFW (Next- Generation Firewall) TIPO I. Especificações Técnicas, suporte técnico 24hrs, monitoramento 24hrs	SERV	2	11.587,48	139.049,76

Grupo	Item	Código CATSER	Especificação	Unidade de Medida	Quantidade	Valor Mensal Total Estimado	Valor Anual Estimado (R\$)
Único	2	27502	Solução de Segurança Cibernética Distribuída NGFW (Next-Generation Firewall) TIPO II. Especificações Técnicas, suporte técnico 24hrs, Monitoramento 24hrs.	SERV	3	4.119,78	49.437,42
	3	27502	Serviço de instalação, configuração, Análise de Cobertura Wireless, e Treinamento de pessoal, para os equipamentos Unifi.	SERV	1	-	8.987,50
	4	27502	Serviço de suporte, e atualização para os equipamentos Unifi	SERV	1	357,50	4.290,00

1.2. Os serviços objeto desta contratação são caracterizados como **comuns**, visto que se enquadram no conceito definido no art. 6º, inc. XIII, da Lei nº 14.133, de 2021.

1.3. O prazo de vigência da contratação é **de 12 (Doze) meses** contados da publicação do Contrato no Portal Nacional de Contratações Públicas - PNCP, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021;

1.4. A presente contratação adotará como regime de execução a **Empreitada de Preço Global por GRUPO**;

1.5. O serviço é enquadrado como continuado tendo em vista que o intuito de garantir a aplicação da política de segurança para adição de dispositivos à rede corporativa do CRM-PB, faz-se necessário realizar a contratação de uma solução de segurança de Firewall que seja capaz de proteger acesso a sites da Internet, reduzir riscos de infecções, redução do consumo do Link Internet, aplicação de regras de firewall definindo os acessos permitidos e bloqueando acessos indevidos Aplicação de regras de IPS para prevenção contra invasões, implementação de VPN (Redes Privadas Virtuais), além de permitir acesso remoto às informações internas somente para pessoal autorizado. Firewall é uma solução de segurança que controla o acesso entre servidores e estações locais de uma rede local e as conexões oriundas ou destinadas à internet. É composto por hardware e software que permitem a aplicação de políticas de acesso, definidas com base na política de segurança, normativos e necessidades de acesso aos dispositivos conectados pelo firewall. Considerando a importância de uma infraestrutura de rede integrada, segura e eficiente, é fundamental que a empresa contratada para prestar suporte ao firewall também assume o suporte técnico dos equipamentos UniFi utilizados em nossa rede. Essa unificação tem como objetivo centralizar o atendimento, facilitar a integração entre os dispositivos, garantir maior agilidade na resolução de incidentes e assegurar uma visão completa da infraestrutura por uma única equipe especializada. Dessa forma, buscamos um parceiro que possa oferecer suporte abrangente, contemplando tanto os dispositivos de segurança quanto os equipamentos de conectividade UniFi, com serviços como monitoramento contínuo, manutenção preventiva, resolução de falhas e suporte evolutivo. Isso garantirá uma operação mais coesa, confiável e eficiente da nossa rede corporativa. É importante destacar que, diferentemente do serviço de firewall — no qual todos os equipamentos serão fornecidos pela empresa contratada — no caso do suporte aos equipamentos UniFi, já possuímos toda a infraestrutura necessária instalada. Assim, o escopo desse serviço será focado exclusivamente no suporte técnico especializado, incluindo monitoramento, manutenção preventiva, resolução de falhas e otimizações. Caso surja a necessidade de substituição ou aquisição de novos equipamentos UniFi, a empresa prestadora do suporte terá apenas o papel de orientar tecnicamente quanto à melhor solução, sem responsabilidade pelo fornecimento dos dispositivos. Reforçamos ainda a importância de que o suporte ao firewall e aos equipamentos UniFi seja realizado por uma única empresa, a fim de garantir maior integração, agilidade no atendimento e eficiência na gestão da infraestrutura de rede.

Sendo a vigência plurianual mais vantajosa considerando a justificativa pormenorizada em tópico específico do Estudo Técnico Preliminar - ETP.

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

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico, constantes nos itens 3 e 7 e respectivos subitens do Estudo Técnico Preliminar - ETP, apêndice deste Termo de Referência;

2.2. O objeto da contratação está previsto no Plano de Contratações Anual de 2025, conforme consta das informações básicas deste termo de referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares no item 6, apêndice deste Termo de Referência.

4. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade:

4.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.1.1. Adoção de critérios ambientais, sociais e econômicos nas contratações, considerando todo o ciclo de vida dos produtos ou serviços;

4.1.2. Preferência por produtos e serviços que apresentem menor impacto ambiental e social;

4.1.3. Estímulo à inovação tecnológica e à adoção de práticas sustentáveis pelos fornecedores;

4.1.4. Transparência e publicidade nas contratações, incluindo a divulgação dos critérios de seleção e avaliação dos fornecedores;

4.1.5. Soluções que viabilizem o incentivo ao desenvolvimento de sistemas de gestão ambiental e empresarial voltados para a melhoria dos processos produtivos e ao reaproveitamento dos resíduos sólidos, incluídos a recuperação e o aproveitamento energético;

Indicação de marcas ou modelos ([Art. 41, inciso I, da Lei nº 14.133, de 2021](#)):

4.2. Na presente contratação não será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s).

Da vedação de utilização de marca/produto na execução do serviço

4.8 Na presente contratação não será admitida a vedação de marca(s), característica(s) ou modelo(s).

Da subscrição e licenciamento oficial do fabricante

4.9 Em caso de fornecedor, revendedor ou distribuidor, será exigido que o produto entregue possua subscrição/suporte oficial e ativo do fabricante durante toda a vigência do contrato, com comprovação exigida no ato do recebimento do equipamento.

Subcontratação

4.3. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

4.4. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#);

Vistoria

4.5. Para o correto dimensionamento e elaboração da sua proposta, o licitante poderá realizar vistoria nas instalações do local onde serão instalados os equipamentos do objeto dessa licitação, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09:00 horas às 16:00 horas, agendada através do e-mail: licitacao@crmpb.org.br.

4.6. O prazo para vistoria iniciar-se-á no dia útil seguinte da publicação do Edital, estendendo-se até o penúltimo dia anterior à data da abertura da sessão pública.

4.7. Para vistoria o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para realização da vistoria.

4.8. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus dos serviços decorrentes.

4.9 A licitante deverá declarar que tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

Da proteção de dados pessoais (LGPD)

4.10. Considerando que a solução de NGFW realiza inspeção de tráfego de rede que pode conter dados pessoais e dados pessoais sensíveis (na acepção dos arts. 5º, I e II, da Lei nº 13.709/2018 — LGPD) tratados pelo CRM-PB no exercício de suas competências legais, ficam estabelecidas as seguintes cláusulas, vinculantes durante toda a vigência contratual:

- 4.10.1. Qualificação da contratada como operadora de dados pessoais (art. 5º, VII, LGPD), com observância de instruções formais do CRM-PB na qualidade de controladora (art. 5º, VI, LGPD);
- 4.10.2. Deveres de confidencialidade, segurança e prevenção a incidentes, nos termos dos arts. 46 a 49 da LGPD;
- 4.10.3. Dever de comunicação imediata, e em prazo nunca superior a 48 (quarenta e oito) horas, de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48 da LGPD);
- 4.10.4. Direito de auditoria do CRM-PB sobre as práticas de tratamento de dados pessoais da contratada, mediante notificação prévia razoável;
- 4.10.5. Jurisdição brasileira para armazenamento de logs e tratamento de dados, vedada a transferência internacional sem autorização específica e formal do CRM-PB;
- 4.10.6. Portabilidade e reversibilidade dos dados ao final da vigência contratual, com prazo certo para devolução em formato estruturado ou eliminação segura, conforme determinação da controladora.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1. Os serviços serão prestados no(s) seguinte(s) endereço(s): Av. Dom Pedro II, 1335 – Centro, CEP. 58.013-420, João Pessoa/PB.

5.2. Os serviços serão prestados no seguinte horário: 07h00min às 17h00min, de segunda à sexta-feira (dias úteis).

Rotinas a serem cumpridas

5.3. A solução especializada em segurança de rede deverá realizar as funcionalidades abaixo requeridas:

5.3.1. Ser do tipo APPLIANCE. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

5.3.2. Garantir que um único equipamento possa atender a totalidade das capacidades exigidas, não sendo aceitos somatórios para atingir os limites mínimos;

5.3.3. Monitoramento da atividade da rede em busca de tráfego com comportamento ou conteúdo malicioso, devendo possuir quantidade de memória e processamento suficientes para atendimento de todas as funcionalidades e desempenho, de acordo com a velocidade do acesso;

5.3.4. Garantir que a solução disponibilize no(s) equipamento(s), acesso a gerência e monitoração, reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões (plataforma com funcionalidades de Next Generation Firewall - NGFW);

5.3.5. Permitir na solução, monitorar via protocolo SNMP, falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, ataques e estatísticas de uso das interfaces de rede;

5.3.6. Garantir o envio dos logs para os sistemas de monitoramento de forma simultânea ou programada;

5.3.7. Garantir que o gerenciamento da solução suporte acesso via SSH, software cliente ou WEB (HTTPS), devendo suportar e garantir o acesso via base de usuários LDAP e LDAP/AD.

5.3.8. Prover filtro de conteúdo Web. Este serviço deve filtrar as requisições de clientes para sites na internet podendo bloquear o acesso do usuário baseado em categorias proibitivas, associados aos crimes cibernéticos como conteúdo sobre pedofilia, pornografia, racismo, e demais conteúdos improdutivos ao trabalho incluindo todos os delitos cibernéticos em geral.

5.3.9. Alertar e registrar estes eventos para futuras análises e ações;

5.3.10. Detectar tráfego que comprometa a segurança e a confiança dos sistemas, tipo ataques contra serviços vulneráveis, comprometimento da integridade, confidencialidade e autenticidade dos sistemas como também a propagação de malwares (vírus, cavalos de tróia, worms e outros),

5.3.11. Permitir, em alguns casos, bloquear ou prevenir tentativa de ataque em tempo real, fazendo o controle baseado em segurança via Firewall.

5.4. A CONTRATADA deverá disponibilizar, para efeito de instalação da solução proposta, sua garantia e prestação dos serviços, incluindo manutenção corretiva, preventiva, atendimento on-site para cidade de João Pessoa, Campina Grande, Patos e Cajazeiras e treinamento, uma equipe com perfil técnico adequado às atividades previstas, com para a operação e configuração de todos os componentes ofertados.

5.5. Os serviços deverão prever todos os equipamentos, componentes e

subcomponentes, objetivando garantir a total conectividade e interoperabilidade, que deverão resultar no perfeito funcionamento do conjunto, com níveis de desempenho adequados aos fins a que se destinam no contexto de melhorias nos Serviços de TIC da CRM-PB.

5.6. Os equipamentos poderão ser enviados pré-configurados para a Sede e as delegacias mencionadas na tabela de localidades. A instalação física e as interconexões junto com o suporte e as orientações da equipe técnica da CONTRATADA.

5.7. A responsabilidade pelo deslocamento de seus técnicos às unidades do CRM-PB, para manutenção dos equipamentos, incluindo retirada e/ou entrega, será exclusiva da CONTRATADA. Isso abrange todas as despesas relacionadas a transporte, frete e seguro.

5.8. Caso a CONTRATADA necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente neste Termo de Referência, mas necessários para atender as funcionalidades exigidas, o custo desses deverão estar inseridos no preço total ofertado.

5.9. Todos os componentes e subcomponentes deverão ser novos, de primeiro uso, sem previsão de descontinuidade anunciada, não se admitindo peças já usadas, reparadas, entre outros, com tecnologia atualizada e avançada, em linha de produção atendendo às características técnicas.

Da execução qualificada — certificação técnica do fabricante

5.9. Todo serviço de suporte ao firewall — em especial a configuração de Alta Disponibilidade da sede — deverá ser executado por profissional com certificação técnica oficial emitida pelo fabricante da solução efetivamente fornecida, em conformidade com as exigências de qualificação técnica detalhadas no item 9 deste Termo e fundamentadas no item 4.7 do Estudo Técnico Preliminar.

5.10. A exigência de certificação não vincula fabricante específico, sendo aceita certificação oficial emitida por qualquer fabricante do segmento NGFW corporativo cuja solução tenha sido ofertada e atenda aos requisitos técnicos deste Termo.

Treinamento

5.11. A CONTRATADA deverá realizar treinamento para os colaboradores da CONTRATANTE, bem como, fornecimento de manuais e boletins técnicos com informações que assegurem a plena utilização dos produtos licenciados sem custo adicional para o CRM-PB. O objetivo é transmitir conhecimentos básicos e funcionais do Firewall.

Níveis de serviço (SLA)

5.11. A LICITANTE deve prever os seguintes Níveis de Serviços:

5.11.1. Plantão técnico de suporte de atendimento: 24 x 7 x 365;

5.11.2. Plantão técnico de suporte on-site: 24 x 7 x 365, para João Pessoa;

5.11.3. Atendimento técnico para análises, alterações de parâmetros, consulta e suporte geral em até 24 (vinte e quatro) horas.

5.12. A LICITANTE não poderá transferir a outrem os compromissos assumidos, no todo ou em parte dos serviços objeto desta contratação.

5.13. Ao final de cada intervenção, a CONTRATADA deve entrar em contato com o CRM-PB para que este proceda com a homologação dos serviços realizados.

5.14. Para facilitar os procedimentos do CRM-PB, a CONTRATADA deve apresentar planilhas específicas, para cada local que foi objeto de intervenção, constando relação detalhada dos produtos efetivamente instalados, dos desempenhos esperados e especificação dos procedimentos técnicos e, se couber, dos instrumentos usualmente adotados para se efetuar os testes.

5.15. Durante todo o período de garantia contratado, o serviço de suporte deve ser suprido 24 (vinte e quatro) horas, 07 (sete) dias por semana.

5.16. A CONTRATADA deve disponibilizar acesso ao ambiente WEB do fabricante para download de arquivos e drivers.

5.17. Todo serviço de suporte do firewall deve ser realizado por profissional certificado pelo fabricante.

5.18. O serviço de suporte deve proporcionar a interação com a equipe técnica do CRM-PB, fornecendo apoio na resolução de incidentes que envolvam os componentes da solução, garantindo seu pronto reestabelecimento.

5.19. Ao final da execução dos serviços pela CONTRATADA, deverão ser realizados todos os testes necessários para comprovar que as instalações estão em condição de funcionar corretamente e de acordo com as especificações e normas.

5.20. Os serviços de SUPORTE TÉCNICO compreendem o diagnóstico e identificação de problemas na solução de firewall, customização de configuração e apoio técnico na utilização da ferramenta;

5.21. A prestação do suporte técnico não poderá haver limites no quantitativo de atendimentos e abertura de chamados;

5.22. Os chamados deverão ter opção de abertura através de portal WEB, E-MAIL telefone 0800 e ligação local, sendo o atendimento em língua portuguesa;

5.23. A CONTRATADA deverá oferecer manutenção e suporte técnico conforme o nível de severidade de cada chamado e dentro dos tempos de resposta definidos abaixo.

5.24. Quando um chamado for aberto pela CONTRATANTE, a CONTRATADA deverá atribuir ao chamado o nível de severidade de acordo com a avaliação do tipo do problema e do impacto/dano.

5.25. Nível de severidade - Descrição de suporte e operações, exemplos:

5.25.1. Severidade A (Crítica): Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impacto sobre a produção ou as atividades da instituição. Vários usuários ou serviços são afetados.

5.25.2. Severidade B (Alta): O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.

5.25.3. Severidade C (Não Crítica): A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável.

5.26. Quanto ao tempo de resposta inicial do suporte técnico, deverá ser baseado nos níveis de severidade descritos acima e no tipo de assinatura contratada. A tabela abaixo descreve as metas de tempo de resposta.

5.27. Nível de severidade - Nível de serviço

Item e Nível de Prestação de Serviço (SLA)	Limites	Valor Acordado Para Aplicação de Descontos nas Faturas por Serviço
Disponibilidade do Firewall	Disponibilidade $\geq$ 99,50% do tempo no mês	Multa de 1% de redução no valor mensal da próxima fatura por cada 0,1% de decréscimo na disponibilidade do serviço. Limitado a 5%.
Atendimento - Severidade A (Crítica)	Disponível: 24/7 Tempo máximo de resposta: duas horas.	0,50% de redução no valor mensal da fatura por cada 30 minutos de atraso excedidos no tempo de resposta. Limitado a 5%.
Atendimento - Severidade B (Alta)	Disponível: 24/7 Tempo máximo de resposta: 24 horas.	0,25% de redução no valor mensal da fatura por cada 2 horas de atraso excedidas no tempo de resposta. Limitado a 3%.
Atendimento - Severidade C (Não Crítica)	Disponível: 24/7 Tempo máximo de resposta: definido no momento da ocorrência entre as partes, mas não superior a 4 dias corridos.	0,25% de redução no valor mensal da fatura por cada dia de atraso excedido no tempo de resposta. Limitado a 2%.

5.28. Os serviços serão prestados de acordo com a tabela abaixo:

Localidade	Endereço	CEP	Quantidade de Firewall
João Pessoa	Rua Dom Pedro II, 1335 - Centro	58040-440	02 Tipo I
Campina Grande	Rua Desembargador Trindade, 173 - Centro	58400-260	01 Tipo II
Patos	Rua Fenelon Bonavides, 211, Sala 202 - Brasília	58700-340	01 Tipo II
Cajazeiras	Rua Victor Jurema, 28 - Centro	58900-000	01 Tipo II

ITEM 01 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW (NEXT-

GENERATION FIREWALL) - TIPO I.

5.29. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, Apple OS ou GNU/Linux.

5.30. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

5.31. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD- WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), Controle de Aplicações, retenção de log.

5.32. Deve possuir retenção de logs em cloud dos últimos 365 dias.

5.33. Deve possuir fonte de alimentação redundante com chaveamento automático 110/220V. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.

5.34. Deve possuir firewall com capacidade mínima de processamento de 09 (nove) Gbps.

5.35. Deve possuir IPS com capacidade mínima de processamento de 2.6 () Gbps.

5.36. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 01 (um) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus atividades maneira simultâneas.

5.37. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 01 (um) Gbps.

5.38. Deve possuir VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec.

5.39. Deve suportar 1.000.000 (um milhão) conexões simultâneas

5.40. Deve suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.

5.41. Deve suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.

5.42. Deve suportar, pelo menos, 10.000 (dez mil) túneis de VPN Client-Site.

5.43. Deve possuir, pelo menos, 02 (dois) interfaces SFP+ 10GE.

5.44. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.

5.45. Deve possuir, pelo menos, 14 (quatorze) interfaces RJ 45.

5.46. Deve incluir licença para a funcionalidade de VPN SSL.

5.47. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

5.48. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

5.49. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

ITEM 02 - SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW (NEXT-GENERATION FIREWALL) - TIPO II

5.50. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, Apple OS ou GNU/Linux.

5.51. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

5.52. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD- WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), Controle de Aplicações, retenção de log(Logs pelo período de 36 meses).

5.53. Deve manter retenção de logs em cloud dos últimos 365 dias.

5.54. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

5.55. Deve possuir firewall com capacidade mínima de processamento de 5 (cinco) Gbps.

5.56. Deve possuir IPS com capacidade mínima de processamento de 800 (oitocentos) Mbps.

5.57. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

5.58. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps.

5.59. Deve possuir VPN com capacidade de, pelo menos, 04 (quatro) Gbps de tráfego IPSec.

5.60. Deve suportar 600.000 (seiscentos mil) conexões simultâneas.

5.61. Deve suportar, pelo menos, 30.000 (trinta mil) novas conexões por segundo.

5.62. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

5.63. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Client-Site.

5.64. Deve possuir, pelo menos, 05 (cinco) interfaces RJ 45.

5.65. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

5.66. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

5.67. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS COMUNS A TODOS OS MODELOS ACIMA (SOLUÇÃO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA NGFW (NEXT- GENERATION FIREWALL) TIPO “I” E “II”)
FUNCIONALIDADE DE FIREWALL

- 5.68.** Deve possuir controle de acesso à internet por endereço IP de origem e destino;
- 5.69.** Deve possuir controle de acesso à internet por sub rede;
- 5.70.** Deve suportar tags de VLAN (802.1q);
- 5.71.** Deve possuir ferramenta de diagnóstico do tipo tcpdump;
- 5.72.** Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
- 5.73.** Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- 5.74.** Deve suportar single-sign-on para Active Directory, RADIUS;
- 5.75.** Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- 5.76.** Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
- 5.77.** Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- 5.78.** Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
- 5.79.** Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- 5.80.** Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
- 5.81.** Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 5.82.** Deve suportar aplicações multimídia, como: H.323 e SIP;
- 5.83.** Deve possuir tecnologia de firewall do tipo Statefull;
- 5.84.** Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo- Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 5.85.** Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;
- 5.86.** Deve suportar PBR – Policy Based Routing;
- 5.87.** Deve permitir a criação de VLANS no padrão IEEE 802.1q;
- 5.88.** Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
- 5.89.** Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
- 5.90.** Deve permitir forwarding de camada 2 para protocolos não IP;

- 5.91.** Deve suportar forwarding multicast;
- 5.92.** Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;
- 5.93.** Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
- 5.94.** Deve permitir o agrupamento de serviços
- 5.95.** Deve permitir o filtro de pacotes sem a utilização de NAT;
- 5.96.** Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas
- 5.97.** Deve possuir mecanismo de anti-spoofing;
- 5.98.** Deve permitir criação de regras definidas pelo usuário;
- 5.99.** Deve permitir o serviço de autenticação para tráfego HTTP e FTP;
- 5.100.** Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;
- 5.101.** Deve possuir a funcionalidade de balanceamento e contingência de links;
- 5.102.** Deve suportar sFlow;
- 5.103.** O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos
- 5.104.** (peer-to-peer) e de mensagens instantâneas.
- 5.105.** Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
- 5.106.** Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 5.107.** Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
- 5.108.** Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
- 5.109.** Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
- 5.110.** Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
- 5.111.** Deve suportar SIP, H.323 e SCCP NAT Traversal;
- 5.112.** Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
- 5.113.** Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- 5.114.** Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações
- (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- 5.115.** Deve permitir modificação de valores DSCP para o DiffServ;
- 5.116.** Deve permitir priorização de tráfego e suportar ToS;
- 5.117.** Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
- 5.118.** Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 5.119.** Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- 5.120.** Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- 5.121.** Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação
- 5.122.** Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;
- 5.123.** Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

- 5.124.** Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
- 5.125.** Deve possuir filtragem de e-mail por palavras chaves;
- 5.126.** Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- 5.127.** Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL
- 5.128.** Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

- 5.129.** Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;
- 5.130.** Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
- 5.131.** Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites

internet Web já registrados e classificados;

5.132. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

5.133. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

5.134. Proxy anônimo;

5.135. Webmail;

5.136. Instituições de saúde;

5.137. Notícias;

5.138. Phishing;

5.139. Hackers;

5.140. Pornografia;

5.141. Racismo;

5.142. Websites pessoais;

5.143. Compras;

5.144. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

5.145. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

5.146. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

5.147. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

5.148. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

5.149. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

5.150. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

5.151. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

5.152. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java e cookies, através de base de URL própria atualizável;

5.153. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

5.154. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

5.155. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

5.156. Deve filtrar o conteúdo baseado em categorias em tempo real;

- 5.157.** Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
- 5.158.** Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- 5.159.** Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 5.160.** Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem; Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
- 5.161.** Deve permitir o bloqueio de redirecionamento HTTP;
- 5.162.** Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
- 5.163.** Deve possuir Proxy Explícito e Transparente;
- 5.164.** Deve implementar roteamento WCCP e ICAP;

FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

- 5.165.** Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- 5.166.** Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas; **5.167.** Deve estar orientado à proteção de redes;
- 5.168.** Deve permitir funcionar em modo transparente, sniffer e router;
- 5.169.** Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- 5.170.** Deve permitir a criação de padrões de ataque manualmente;
- 5.171.** Deve possuir integração à plataforma de segurança;
- 5.172.** Deve possuir capacidade de remontagem de pacotes para identificação de ataques;
- 5.173.** Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
- 5.174.** Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como **5.175.** Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 5.176.** Deve possuir mecanismos de detecção/proteção de ataques;
- 5.177.** Deve possuir reconhecimento de padrões; **5.178.** Deve possuir análise de protocolos; **5.179.** Deve possuir detecção de anomalias;
- 5.180.** Deve possuir detecção de ataques de RPC (Remote Procedure Call); **5.181.** Deve possuir proteção contra-ataques de Windows ou NetBios;
- 5.182.** Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

- 5.183.** Deve possuir proteção contra-ataques DNS (Domain Name System); 5.184. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- 5.185.** Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol); 5.186. Deve possuir métodos de notificação de detecção de ataques;
- 5.187.** Deve possuir alarmes na console de administração; 5.188. Deve possuir alertas via correio eletrônico;
- 5.189.** Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- 5.190.** Deve ter a capacidade de resposta/logs ativa a ataques;
- 5.191.** Deve prover a terminação de sessões via TCP resets;
- 5.192.** Deve armazenar os logs de sessões;
- 5.193.** Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 5.194.** Deve mitigar os efeitos dos ataques de negação de serviços;
- 5.195.** Deve permitir a criação de assinaturas personalizadas;
- 5.196.** Deve possuir filtros de ataques por anomalias;
- 5.197.** Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 5.198.** Deve permitir filtros de anomalias de protocolos;
- 5.199.** Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- 5.200.** Deve suportar verificação de ataque na camada de aplicação;
- 5.201.** Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;
- 5.202.** Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

FUNCIONALIDADE DE VPN

- 5.203.** Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 5.204.** Deve possuir suporte a certificados PKI X.509 para construção de VPNs;
- 5.205.** Deve possuir suporte a VPNs IPSec Site-to-Site e VPNs IPSec Client-to-Site;
- 5.206.** Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
- 5.207.** Deve permitir a arquitetura de VPN hub and spoke;
- 5.208.** Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- 5.209.** Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;
- 5.210.** Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
- 5.211.** Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
- 5.211.1.** P2P
 - 5.211.2.** Instant Messaging;
 - 5.211.3.** Web client;
 - 5.211.4.** Transferência de arquivos;
 - 5.211.5.** VoIP;
- 5.212.** Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 5.213.** Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma.
- 5.214.** Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 5.215.** Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- 5.216.** Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- 5.217.** Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- 5.218.** Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 5.219.** Deve possuir integração com tokens para autenticação de 02 (dois) fatores;
- 5.220.** Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
- 5.221.** Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
- 5.222.** Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
- 5.223.** Deve permitir criação de padrões de aplicação manualmente;

FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

- 5.224.** Deve permitir a criação de endereços IPs virtuais;
- 5.225.** Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;
- 5.226.** Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP,

HTTPS, TCP e UDP;

5.227. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

5.228. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

5.229. Deve permitir que seja mantido o IP de origem;

5.230. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários.

5.231. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

5.232. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

FUNCIONALIDADE DE VIRTUALIZAÇÃO

5.233. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

5.234. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

5.235. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

FUNCIONALIDADE DE SD-WAN

5.236. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

5.237. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

5.238. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

5.239. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

5.240. Solução deve ser capaz de prover Zero Touch provisioning.

5.241. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

5.242. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

5.243. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI,

de forma automática, e sem que o administrador precise configurar site por site.

5.244. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.

5.245. Reconhecimento em camada 7 totalmente segregado da camada 4.

5.246. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

5.247. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

5.248. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc)

5.249. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

5.250. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD- WAN em condições onde a largura de banda é modificada.

5.251. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

5.252. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de saúde melhor que o link atual

5.253. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

5.254. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

ITEM 03 - SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO, ANÁLISE DE COBERTURA WIRELESS, E TREINAMENTO DE PESSOAL, PARA OS EQUIPAMENTOS UNIFI

5.255. Entre os equipamentos estão:

5.255.1. 3 UniFi Switch 48 500W 48 Ports Giga RJ45 Ethernet 1G SFP ;

5.255.2. 2 Ports 10G SFP +1 Switch Standard 48 portas 10/100/1000 USW-48 Ubiquiti;

5.255.3. 1 Unifi Security Gateway Pro USG Pro 4;

5.255.4. 9 AP Unifi AC Lite;

5.255.5. 6 Access Point UAP-AC-HD Throughput até 2.5 Gbps (Bandas de 2.4/5 GHz) PoE+ Adapter 48 VDC U-POE-at-BR

5.256. Consiste em fornecer serviços de suporte à solução de rede local existente atualmente na sede do CRM-PB em João Pessoa, assim como remoto para as localidades de Campina Grande, Patos e Cajazeiras.

5.257. O objetivo deste suporte é que uma única empresa cuide tanto do parque atualmente existente, quanto da cibersegurança, facilitando a configuração e integração da rede. A CONTRATADA não será responsável pelo fornecimento de equipamentos neste serviço, apenas configuração e operação. Caso surja a necessidade de substituição ou aquisição de novos equipamentos UniFi, a empresa prestadora do suporte terá apenas o papel de orientar tecnicamente quanto à melhor solução, sem responsabilidade pelo fornecimento dos dispositivos.

5.258. A CONTRATADA deverá realizar as seguintes atividades para implantação do parque atual: Integração com o firewall, garantindo o pleno funcionamento e a compatibilidade entre os sistemas de rede e segurança.

5.259. Realização de site survey para analisar a melhor localização dos Pontos de Acesso (APs) listados no item anterior, garantindo a melhor cobertura e baixa interferência

5.260. Instalação e configuração inicial do parque existente, descrito no item acima, e sua sincronização junto à solução de segurança

5.261. Configurar visualização e gestão dos Pontos de Acesso (APs e switches das delegacias através da sede, como é feito atualmente.

5.262. Criação e administração de dois segmentos de rede Wi-Fi independentes na mesma estrutura física:

5.262.1. Rede 1, interna, integrada à rede local do Conselho, com acesso ao Active Directory e servidores;

5.262.2. Rede 2, internet, somente para acesso à internet por visitantes;

5.262.3. A implantação e configuração iniciais do parque atual deverá ser realizada localmente nas unidades do CRM-PB.

ITEM 04 - SERVIÇO DE SUPORTE, E ATUALIZAÇÃO PARA OS EQUIPAMENTOS UNIFI

5.263. Após a implantação e configuração iniciais, a CONTRATADA deverá realizar as seguintes atividades para Operação e manutenção do parque atual:

5.263.1. Realização eventuais ajustes na configuração, de maneira remota, caso seja demandado pela equipe de TI do CRM PB;

5.263.2. Fornecimento de suporte integrado, conforme descrito no item de Monitoramento dos Serviços e Gerência Proativa;

5.263.3. Realização de atualização de firmwares e patches de segurança do parque descrito neste capítulo sempre que necessário.

5.264. As atividades de operação e manutenção do parque atual devem ser realizadas remotamente, sendo que caso seja necessária alguma manobra local, a equipe de manutenção da CONTRATADA poderá orientar um técnico do CRM-PB para sua execução, deslocando técnico próprio ao local apenas caso seja necessário.

5.265. A implantação, configuração inicial, operação e manutenção do parque atual devem ser realizadas por profissionais com comprovado conhecimento técnico e experiência nos equipamentos utilizados, descritos acima, garantindo a execução adequada das atividades e a continuidade dos serviços de rede do CRM PB.

5.266. Suporte e garantia consistem em um serviço de prestação de assistência intelectual, tecnológica e material os itens da solução sob cobertura contratual, complementada pela garantia da operacionalidade dos equipamentos por meio de troca/substituição de componentes em falhas do firewall e atualizações de firmware/software embarcados para correção de falhas e aprimoramento dos requisitos de segurança da informação.

5.267. A CONTRATADA deverá disponibilizar Central de atendimento para recebimento e registro da demanda do CONTRATANTE em regime 24 x 7, ou seja, 24 horas contínuas do dia, em todos os dias da semana. O registro dos chamados deverá ser identificado por número de protocolo e informado ao CONTRATANTE.

5.268. Na hipótese de riscos de descontinuidade operacional dos equipamentos envolvidos no atendimento, devido à necessidade de aplicação de solução de correção ou atualização, a intervenção técnica poderá ser agendada fora de horário comercial.

5.269. Durante todo o período de suporte técnico, a CONTRATADA deverá garantir o funcionamento da solução e deverá prestar serviços de assistência técnica por meio de manutenção preventiva, manutenção corretiva, sem ônus para o CONTRATANTE.

5.270. A CONTRATADA poderá realizar manutenções preventivas a pedido do CONTRATANTE ou por iniciativa própria desde que se estabeleça junto ao CONTRATANTE um agendamento prévio para tais atividades.

5.271. Caberá ao CRM-PB requisitar o suporte técnico, ficando a CONTRATADA obrigada a realizá-lo, nos prazos máximos definidos.

5.272. A solução para o defeito apresentado na solução deverá ser realizada por técnico especializado que efetuará a configuração ou reparação do equipamento para o seu pleno funcionamento.

5.273. Entende-se por término de atendimento a disponibilidade do equipamento para uso em perfeitas condições de funcionamento no local onde está instalado, juntamente com o recebimento, pela CONTRATANTE, do relatório técnico de atendimento emitido pela CONTRATADA.

5.274. O relatório técnico de atendimento emitido pela CONTRATADA deverá conter, no mínimo: data e hora da solicitação, do início e do término do atendimento, identificação do problema e providências adotadas, além das demais informações pertinentes.

5.275. O relatório técnico de atendimento deverá ser enviado ao CONTRATANTE, pela CONTRATADA, via correio eletrônico por representante técnico ou preposto da CONTRATADA.

5.276. A CONTRATADA deverá prestar todas as informações solicitadas pelo CONTRATANTE sobre o andamento do atendimento do suporte e de garantia imediatamente ao ser solicitado.

5.277. Para a execução de atendimento de instalação ou desinstalação de quaisquer soluções ou equipamentos, é necessária autorização da CONTRATANTE.

5.278. É garantido à CONTRATADA o direito de contestação dos resultados da apuração dos tempos para atendimento do serviço de suporte técnico, bem como de apresentar as justificativas que se fizerem necessárias.

5.279. Regras para o serviço de atendimento do serviço de suporte técnico envolvendo resolução de incidentes e/ou problemas:

5.279.1. Regras e prazos para o serviço de suporte técnico uma vez constatada

necessidade de configuração da solução, ajustes e reinstalação da solução

5.279.2. Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA, para acompanhamento e controle da execução do serviço.

5.279.3. A CONTRATADA deverá dispor de equipe técnica qualificada para a prestação de todos os serviços técnicos previstos neste Termo de Referência.

5.279.4. Os serviços técnicos deverão sempre ser executados por profissionais que detenham os conhecimentos requeridos para a execução dos serviços detalhados em Ordem de Serviços ou Chamados Técnicos.

5.279.5. A execução dos serviços técnicos deverá ser realizada pela CONTRATADA ou diretamente pelo fabricante com acompanhamento e supervisão da área técnica do CONTRATANTE.

5.279.6. O serviço de suporte técnico deverá ser prestado no idioma português;

5.279.7. Caso a CONTRATADA não consiga executar a Ordem de Serviço ou Chamado Técnico conforme as condições demandadas, deverá comunicar ao fiscal por escrito, justificando os fatos e motivos que impediram sua execução, cabendo ao gestor acatar ou não a justificativa.

5.280. A CONTRATADA deverá realizar a verificação da qualidade antes da entrega dos produtos gerados, visando artefatos livres de defeitos e de desconformidades. O CONTRATANTE também realizará a sua verificação da qualidade com vistas ao aceite dos produtos gerados pela CONTRATADA, utilizando os critérios de aceitação inclusos de acordo com cada Chamado Técnico.

5.281. Os casos de atrasos deverão ser motivados, explicando as razões que os fundamentaram.

5.282. Versões eletrônicas de todos os artefatos envolvidos no Chamado Técnico (quando possível) devem ser entregues à Fiscalização.

5.283. Os atrasos não justificados ou não aceitos pela fiscalização do contrato estarão sujeitos à aplicação das sanções cabíveis.

Materiais a serem disponibilizados

5.284. Para a realização dos serviços, todos os insumos que porventura sejam necessários, deverão ser fornecidos pela Contratada;

5.285. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Procedimentos de transição e finalização do contrato

5.286. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

5.286.1. Transferência de Dados e Documentos: A CONTRATADA deve repassar ao CONTRATANTE e/ou à nova contratada todos os dados, documentos e elementos de informação que foram utilizados ou gerados durante a execução dos serviços. Isso

inclui, mas não se limita a configurações de sistemas, registros de incidentes, logs de segurança, e relatórios de desempenho.

5.286.2. Debriefing e Revisões Finais: Realização de reuniões de debriefing com as equipes relevantes do CRM-PB e da nova contratada, se aplicável, para discutir os aspectos operacionais, desafios enfrentados e lições aprendidas durante o contrato.

5.286.3. Transferência de Conhecimento: Serão organizadas sessões de transferência de conhecimento e capacitação para as equipes do CRM-PB e/ou da nova contratada para garantir que haja entendimento completo dos processos, procedimentos e particularidades das soluções implementadas.

5.286.4. Desmobilização de Recursos: Planejamento e execução eficaz da desmobilização de recursos da CONTRATADA, incluindo a retirada de equipamentos (se aplicável) e a desativação de acessos, de forma a não comprometer a segurança e a operação do CRM-PB.

5.286.5. Assistência durante o Período de Transição: Disponibilização de suporte técnico durante um período de transição acordado, para assegurar que quaisquer questões emergentes sejam prontamente atendidas e resolvidas.

5.286.6. Documentação de Encerramento: Preparação de um relatório de encerramento detalhado, incluindo um resumo das atividades realizadas, status das soluções implementadas e recomendações para o futuro.

6. MODELO E GESTÃO DE CONTRATO

6.1. 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;

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. As comunicações entre o órgão ou entidade 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;

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato;

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros;

Rotinas de Fiscalização

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do

contrato, ou pelos respectivos substitutos.

Fiscalização Técnica

6.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

6.8. O fiscal técnico do contrato 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;

6.9. Identificada qualquer inexactidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;

6.10. 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;

6.11. 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;

6.12. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação;

6.13. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

6.13.1. Revisar as contas de acesso administrativo ao firewall e ao controlador Unifi, garantindo que apenas usuários autorizados tenham acesso e que as permissões estejam corretas;

6.13.2. Fiscalizar a criação, modificação e exclusão de acessos VPN, garantindo que as políticas de segurança para acesso remoto sejam seguidas;

6.13.3. Assegurar que o firewall e os dispositivos Unifi (APs, switches, controladores) estejam sempre com as últimas versões de firmware e software, incluindo a aplicação de patches de segurança;

6.13.4. Acompanhar a execução de varreduras de vulnerabilidade e a correção das falhas identificadas nos equipamentos protegidos pelo firewall;

6.13.5. Observar se a resposta a incidentes de segurança (invasões, ataques, tentativas de acesso não autorizado) é rápida, eficaz e segue os procedimentos definidos;

6.13.6. Fiscalizar se todas as alterações nas configurações do firewall e Unifi seguem um processo formal de gestão de mudanças;

6.13.7. Exigir e analisar relatórios de desempenho, segurança e conformidade do firewall e da rede Unifi, que devem ser entregues pelo fornecedor conforme o cronograma contratual;

6.13.8. Verificar se a documentação da infraestrutura de firewall e Unifi (diagramas de rede, configurações, inventário de ativos) está sempre atualizada e acessível;

- 6.13.9.** Avaliar a qualidade do suporte técnico prestado pela equipe do fornecedor, incluindo a comunicação, o conhecimento técnico e a proatividade na resolução de problemas
- 6.13.10.** Entender e fiscalizar o processo de escalonamento de problemas críticos para garantir que as questões sejam tratadas nos níveis adequados de urgência e expertise;
- 6.13.11.** Garantir que os logs do firewall (tráfego permitido/bloqueado, eventos de segurança) e dos dispositivos Unifi (conexões, alertas) estejam sendo coletados, armazenados e analisados adequadamente para auditoria e detecção de anomalias;
- 6.13.12.** Acompanhar métricas de desempenho, como latência, perda de pacotes e uso de largura de banda, para identificar possíveis gargalos ou degradação do serviço;
- 6.13.13.** Confirmar que as bases de assinaturas de IPS/IDS (Sistema de Prevenção/Detecção de Intrusão), antivírus e filtragem de conteúdo do firewall estão sendo atualizadas regularmente; e
- 6.13.14.** Verificar se as regras do firewall e as políticas de segurança da rede Unifi (segmentação de rede, autenticação Wi-Fi, controle de acesso) estão corretamente aplicadas e alinhadas com as diretrizes de segurança da organização.
- 6.14.** A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.
- 6.15.** As disposições previstas neste Termo de Referência não excluem o disposto no Anexo VIII da Instrução Normativa SEGES/MP nº 05, de 2017, aplicável no que for pertinente à contratação, por força da Instrução Normativa Seges/ME nº 98, de 26 de dezembro de 2022.

Fiscalização Administrativa

- 6.16.** O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;
- 6.17.** Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

Gestor do Contrato

- 6.18.** Cabe ao gestor do contrato:

6.18.1. coordenar 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 ordem 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.

6.18.2. acompanhar os registros realizados pelo (s) fiscal (is) 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.

6.18.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

6.18.4. emitir documento comprobatório da avaliação realizada pelo (s) fiscal (is) 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.

6.18.5. tomar providências para a formalização de 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.

6.18.6. 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.

6.18.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1. A avaliação da execução do objeto utilizará o disposto neste item:

7.2. Será indicada a retenção ou glosa do pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.2.1. Não produziu os resultados acordados;

7.2.2. Deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou **7.2.3.** Deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demanda;

7.3. Os serviços serão recebidos provisoriamente, no prazo de 5 (cinco) dias, pelo (s) fiscal (is), mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

7.4. 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 parcela a ser paga.

7.5. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

7.6. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

7.7. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.8. Para efeito de recebimento provisório, ao final de cada período 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 em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.9. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.10. 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 última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.11. A fiscalização não efetuará o ateste da última e/ou única medição de 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)

7.12. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.13. 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.

7.14. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.15. Os serviços serão recebidos definitivamente no prazo de 10 (dez) 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:

7.15.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (Decreto Estadual nº 43.975, de 2023, art. 23, VIII).

7.15.2. 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;

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

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

7.17.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.18. 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 quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

7.20. 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

7.21. 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 art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

7.22. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos 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, de 2021.

7.23. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.23.1. o prazo de validade;

7.23.2. a data da emissão;

7.23.3. os dados do contrato e do órgão contratante;

7.23.4. o período respectivo de execução do contrato;

7.23.5. o valor a pagar; e

7.23.6. eventual destaque do valor de retenções tributárias cabíveis;

7.24. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

7.25. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada 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.

7.26. A Administração deverá realizar consulta ao SICAF para:

7.27. verificar a manutenção das condições de habilitação exigidas no edital;

7.28. identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.29. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, 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.

7.30. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, 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.

7.31. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

Prazo de Pagamento

7.32. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.33. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

Forma de Pagamento

7.34. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

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

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

7.36.1. 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.

7.37. O contratado 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.

Reajuste

7.38. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado.

7.39. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.40. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.41. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.42. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.43. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.44. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.45. O reajuste será realizado por apostilamento.

8. FORMA E CRITÉRIOS DE SELEÇÃO E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

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

Regime de Execução

8.2. O regime de execução do contrato será **POR PREÇO GLOBAL**.

Exigências de habilitação

8.3. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação Jurídica:

8.4. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

8.5. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.6. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/ptbr/empreendedor>;

8.7. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

8.9. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

8.11. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971;

8.12. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021);

8.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação da respectiva Habilitação fiscal, social e trabalhista;

Habilitação fiscal, social e trabalhista

8.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

8.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.18. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.19. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

8.20. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

8.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal;

Qualificação Econômico-Financeira

8.22. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

8.23. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

8.24. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

8.24.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

8.24.2. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

8.24.3. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped;

8.25. As empresas criadas no exercício financeiro da contratação direta deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º);

8.26. A documentação referida na Qualificação Econômico-Financeira constante do item 8.33, 8.34 e seus subitens:

8.27. Deverá ser obrigatória, em razão da contratação não se configurar como entrega imediata, nos termos do art. 70, III da Lei 14.133/21;

Qualificação Técnica:

8.28. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado;

8.29. Todas as especificações do objeto contidas na proposta vinculam o licitante;

8.30. Deverá haver a comprovação da experiência mínima de 01 (um) ano na prestação dos serviços, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os 12 (doze) meses serem ininterruptos. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social:

8.30.1. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução conforme IN SEGES/MP n. 5, de 2017;

8.30.2 Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante.

8.31. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos;

8.32. A comprovação de vinculação do profissional ao licitante será efetuada através da apresentação de cópia autenticada da CTPS, se empregado, contrato de prestação de serviço ou termo de compromisso assinado pelo profissional e pela licitante, se não empregado e, no caso de Sócio, mediante apresentação do contrato social em vigor;

8.33. Declaração de que dispõe de mão-de-obra adequada e disponível, além de local para execução dos serviços técnicos. Deverá ser apresentado, no mínimo, **01 (hum) profissionais técnicos**, integrantes do quadro da empresa sócio e/ou funcionário e/ou prestadores de serviços devidamente treinados pelo fabricante para instalar, configurar e manter os itens ofertados, devendo estes treinamentos técnicos serem comprovados por certificados de qualificação técnica vigentes;

8.34. Declaração de que dispõe de mão-de-obra adequada e disponível, além de local para execução dos serviços técnicos. Deverá ser apresentado, no mínimo, **01 (hum) profissionais técnicos**, integrantes do quadro da empresa sócio e/ou funcionário e/ou prestadores de serviços devidamente treinados pelo fabricante para instalar, configurar e manter os itens ofertados, devendo estes treinamentos técnicos serem comprovados por certificados de qualificação técnica vigentes;

8.35. Visando atender com celeridade às obrigações deste contrato e dada a criticidade do equipamento de segurança (firewall), a contratada deverá garantir força de trabalho suficiente e logística adequada para cumprir o Acordo de Nível de Serviço (SLA) após a abertura do chamado. A comprovação da capacidade para cumprir este prazo, seja por meio de base operacional, rede credenciada ou plano de deslocamento, deverá ser apresentada em até 15 (quinze) dias após a assinatura do contrato, sujeitando-se a contratada às penalidades legais e contratuais cabíveis em caso de descumprimento do tempo de resposta estipulado;

8.35.1. Prospecto com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais

literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico;

8.35.2. Indicação exata do modelo de equipamento ofertado, no Sistema Eletrônico de Disputas e na Proposta de Preços, sendo os respectivos catálogos obrigatoriamente de domínio público, ou seja, deverão estar publicados no website do fabricante, comprovando todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas neste Termo de Referência – Especificações Técnicas;

8.35.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

8.36. Declaração de que o interessado tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da contratação;

8.36.1. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do interessado acerca do conhecimento pleno das condições e peculiaridades da contratação;

8.37. Registro ou inscrição da empresa na entidade profissional competente, em plena validade;

8.38. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;

8.39. O interessado disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de **R\$201.764,68 (duzentos e um mil setecentos e sessenta e quatro reais e sessenta e oito centavos)**, conforme custos unitários apostos no item 01 deste instrumento;

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. As despesas decorrentes da presente contratação, correrão à conta de recursos específicos consignados no Orçamento deste exercício, no qual consta saldo suficiente para o devido atendimento, conforme dotação abaixo discriminada:

6.2.2.1.1.33.90.39.004 - SERVIÇOS TÉCNICOS PROFISSIONAIS - P.J.

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

11. OBRIGAÇÕES DA CONTRATANTE

11.1. São obrigações da CONTRATANTE:

- 11.1.1.** Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 11.1.2.** Receber o objeto da contratação direta no prazo e condições estabelecidas neste Termo de Referência;
- 11.1.3.** Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
- 11.1.4.** Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado, através de comissão e/ou servidor especialmente designado para o feito;
- 11.1.5.** Comunicar a empresa para emissão de Nota Fiscal no que se refere à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;
- 11.1.6.** Efetuar o pagamento a Contratada, no valor correspondente ao objeto da contratação direta entregue ao órgão, desde que no prazo e forma estabelecidos no Termo de Referência;
- 11.1.7.** Aplicar as sanções administrativas, quando se fizerem necessárias;
- 11.1.8.** Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste;
- 11.1.9.** A Administração terá o prazo de 10 (dias), a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período;
- 11.1.10.** Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 15 dias;
- 11.1.11.** Verificar minuciosamente no prazo fixado, a conformidade dos bens fornecidos com as especificações constantes deste Termo de Referência e da proposta, para fins de aceitação e recebimento definitivos;
- 11.1.12.** Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021;
- 11.1.13.** Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
- 11.1.14.** Assegurar que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pelo Contratado, das normas de segurança e saúde no trabalho, quando o serviço for executado em suas dependências, ou em local por ela designado;
- 11.1.15.** O contratante não será responsável por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do presente Termo de Referência, bem como, por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos e/ou subordinados;

12. OBRIGAÇÕES DA CONTRATADA

12.1. São obrigações da contratada

12.1.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

12.1.2. Efetuar entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência;

12.1.3. Atender às determinações regulares emitidas pelo fiscal contratual ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados;

12.1.4. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

12.1.5. Manter-se durante toda a vigência da contratação direta, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para este tipo de contratação;

12.1.6. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato ou documentos que o substituam;

12.1.7. A solicitação de pagamento deverá ser até o limite total do valor da aquisição e acompanhado da respectiva Nota Fiscal;

12.1.8. Responsabilizar-se pelos vícios e danos decorrentes do objeto fornecido, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

12.1.9. Reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto que estiver fora das especificações deste termo de referência, no qual se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados, bem como fora do prazo de validade (Lei nº 14.133/2021, art. 119);

12.1.10. Comunicar à Contratante, 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;

12.1.11. Apresentar a Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução/entrega do objeto;

12.1.12. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

12.1.13. Realizar os serviços de manutenção e assistência técnica na Av. Dom Pedro II, 1355 – Torre – João Pessoa/PB. Cep: 58.040-300.

12.1.14. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

13. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133, de

2021, o Contratado que:

- a)** der causa à inexecução parcial do contrato;
- b)** der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c)** der causa à inexecução total do contrato;
- d)** ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e)** apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f)** praticar ato fraudulento na execução do contrato;
- g)** comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h)** praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;

13.2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

13.2.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei);

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

13.2.3. Declaração de inidoneidade para licitar e contratar quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

13.2.4. Multa:

1) moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;

2) compensatória de 10 % (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

13.3. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º);

13.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º);

13.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157);

13.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º);

13.7. A multa poderá ser recolhida administrativamente no prazo máximo de 30(trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente;

13.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure

o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar;

13.9. Na aplicação das sanções serão considerados (art. 156, §1º):

- a)** a natureza e a gravidade da infração cometida;
- b)** as peculiaridades do caso concreto;
- c)** as circunstâncias agravantes ou atenuantes;
- d)** os danos que dela provierem para o Contratante;
- e)** a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.10. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159);

13.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160);

13.12. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal. (Art. 161);

13.12.1. As penalidades serão obrigatoriamente registradas no SICAF.

13.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21;

13.14. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

14. DAS DISPOSIÇÕES GERAIS

14.1. As informações constantes neste Termo de Referência não são classificadas como sigilosas, **com exceção do custo estimado da contratação**, cujo caráter sigiloso é mantido até o julgamento das propostas;

Submeto o presente Termo de Referência à aprovação do Ordenador de Despesas.

João Pessoa (PB), data da assinatura eletrônica via SEI.

Elaborado por:

Bruno de Lima Silva

Coordenador de TI

Matrícula: 66

Aprovado por:

Bruno Leandro de Souza

Presidente do CRM-PB



Documento assinado eletronicamente por **Bruno de Lima Silva, Coordenador(a) de Informática**, em 01/10/2026, às 15:18, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Bruno Leandro de Souza, Presidente**, em 05/10/2026, às 16:58, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4986411** e o código CRC **775FE4F8**.



Av. Dom Pedro II, 1335 - Bairro Torre |
CEP 58040-440 | João Pessoa/PB -
<https://crmpb.org.br/>



Referência: Processo SEI nº 25.15.000002053-1 | data de inclusão: 01/10/2026