GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Educação - SEDUC
Gerência de Contratações de Serviços - SEDUC-GCS

TERMO DE REFERÊNCIA

RP Nº 126/2025

1. INFORMAÇÕES BÁSICAS:

1.1. **Unidade Orçamentária:** Secretaria de Estado da Educação - SEDUC

1.2. **Unidade Requisitante:** Gerência de Segurança da Informação e Operação de Redes- SEDUC- GSIOR

1.3. **Unidade Solicitante:** Gerência de Planejamento de Contratação de Serviços- SEDUC-GPCS

1.4. **Processo Administrativo:** 0029.003939/2025-74

2. BASE LEGAL:

2.1. O presente Termo de Referência foi elaborado com base no Estudo Técnico Preliminar 47 (70175357), em atendimento ao disposto na Lei Federal 14.133/2021, norma geral e o Decreto Estadual nº 28.874/2024, que regulamenta o Pregão na forma Eletrônica, definindo o conjunto de elementos que nortearão o procedimento licitatório para aquisições de Bens e contratação de serviços.

3. OBJETO:

3.1. Constitui o presente Termo de Referência, o Registro de Preços para a futura e eventual contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações Web da SEDUC-RO, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização, conforme condições, quantidades e exigências estabelecidas neste instrumento.

3.2. **Quadro de Especificações Técnicas dos Itens, Serviços e Quantitativos:**

Grupo	Classe (CATMAT / CATSER)	Item	Detalhamento do objeto	Unidade de Medida	Quantidade
1	481646	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com garantia para 60 meses.	Unidade	4
	27090	2	Licenciamento e garantia da Solução de Firewall de Aplicação Web (Web Application Firewall) com garantia e suporte para 60 meses.	Unidade	4
	27111	3	Serviço de instalação e configuração da Solução de firewall de aplicação Web.	Unidade	4
	27014	4	Manutenção e suporte da Solução de Firewall de Aplicação Web (Web Application Firewall).	Mês	60
	16837	5	Treinamento na solução para (10 participantes).	Unidade	10
	26077	6	Solução de Segurança Avançada, com garantia para 60 meses	Unidade	4

3.3. **Natureza do Serviço:**

3.3.1. Os Serviços Objeto desta Contratação são caracterizados como comum (ns), nos termos do art. 6º, XIII da Lei nº 14.133/21.

3.3.2. A contratação será realizada por meio de licitação, na modalidade Pregão, na sua forma eletrônica, com critério de julgamento por menor preço, nos termos dos artigos 28, I, da Lei Federal nº 14.133/2021.

3.3.3. Nos termos do art. 82, inciso III, da Lei nº 14.133/2021, em análise a possibilidade de adoção de preços diferenciados em razão de circunstâncias específicas relacionadas ao objeto da contratação, conclui-se que não será adotada a previsão de preços diferenciados para a presente contratação, pelos motivos a seguir expostos:

I - O objeto consiste em solução padronizada e integrada de tecnologia da informação, cujos componentes devem operar de forma uniforme e interoperável, não sendo tecnicamente recomendável a variação de preços em função de condições de execução;

II - Os serviços e bens envolvidos apresentam características homogêneas e parâmetros técnicos uniformes, não havendo variação significativa que justifique diferenciação de preços;

III - A contratação será realizada por lote único, contemplando solução completa, o que demanda coerência e uniformidade na formação dos preços;

IV - A adoção de preços diferenciados poderia comprometer a isonomia entre os licitantes e a comparabilidade objetiva das propostas, prejudicando o julgamento pelo critério de menor preço;

V - A estratégia adotada encontra-se alinhada às melhores práticas de contratações de soluções de TIC integradas, priorizando padronização, governança e eficiência operacional.

3.3.4. Dessa forma, justifica-se tecnicamente a não aplicação da previsão de preços diferenciados, por não se mostrar adequada à natureza e às características do objeto contratado.

3.3.5. Para a prestação dos serviços pretendidos os eventuais interessados deverão comprovar que atuam em ramo de atividade compatível com o objeto da licitação, bem como apresentar todos os documentos a título habilitação, nos termos do art. 62, da Lei nº 14.133/2021.

3.3.6. A contratação observará as disposições da LC nº 123/06, no que couber.

3.3.7. Considerando a especificidades do objeto e sua execução, a contratante estima que as quantidades poderão ser acrescidas ou suprimidas em até 25% (vinte e cinco por cento), conforme art. 125 da Lei nº 14.133/2021.

3.3.8. Para esta contratação as licitantes interessadas deverão formular suas propostas considerando 100% (cem por cento) dos quantitativos estipulados por item/lote, nos termos do art. 82, inciso II, da Lei nº 14.133/2021.

3.3.9. Não será admitida a oferta de proposta em quantitativo inferior ao máximo previsto neste TR, conforme dispõe o art. 82, inciso IV, da Lei nº 14.133/2021, sendo que tal permissão poderá incorrer no acréscimo do volume de contratos, por conseguinte, influenciando negativamente no gerenciamento.

3.3.10. Adicionalmente, considerando a natureza integrada da solução de segurança da informação pretendida, composta por fornecimento de equipamentos (appliances), licenças, serviços de instalação, suporte técnico e atualização, não será admitida cotação parcial de quantitativos, sob pena de desclassificação da proposta. A exigência de cotação mínima integral justifica-se pelos seguintes aspectos técnicos e operacionais:

I - A solução objeto da contratação constitui ambiente único e integrado de segurança, cuja efetividade depende da implementação completa de todos os seus componentes;

II - A adoção de quantitativos inferiores comprometeria a arquitetura de alta disponibilidade (cluster entre datacenters principal e secundário), prejudicando a continuidade dos serviços;

III - A prestação dos serviços envolve custos fixos relevantes de mobilização, instalação, parametrização e suporte, tornando inviável a execução para quantitativos reduzidos;

IV - A contratação integral assegura padronização tecnológica, compatibilidade entre os componentes e otimização da gestão da solução;

V - A medida não compromete a competitividade, uma vez que os quantitativos foram definidos com base em estudo técnico preliminar, análise de mercado e contratações similares, conforme demonstrado no item 3.9. deste Termo de Referência.

3.3.11.
Dessa forma, a exigência de cotação mínima integral mostra-se necessária para garantir a viabilidade técnica, a economicidade e a adequada execução contratual.

3.3.12. O serviço é enquadrado como continuado tendo em vista haver necessidade de caráter permanente nas unidades contempladas, para a execução dos serviços a serem desenvolvidos nos moldes programados para execução do objeto, sendo a vigência plurianual mais vantajosa considerando os custos de realização de uma nova contratação e o reajuste por índice oficial de mercado ICTI (Índice de Custos de Tecnologia da Informação).

3.3.13. A execução dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

3.4. **Do Modo de Disputa:**

3.4.1. Será adotado para o envio de lances no pregão eletrônico o modo de disputa **"aberto", em conformidade com art. 42, Inciso XIII e art. 22, Inciso II, da IN 73/2022**.

3.4.2. Em consonância ao inciso I do Art. 56 da Lei nº 14.133, de 2021, no modo de disputa aberto, os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, crescentes ou decrescentes, visto que se trata de um pregão cujo o critério de julgamento é menor preço para os itens/lotes da licitação.

3.4.3. Outrossim, no modo de disputa aberto, a fase de lances resume-se à disputa eletrônica, realizada por todos os licitantes, oportunidade em que os valores são registrados pelo sistema e o lance vencedor é aquele que contém o melhor preço, obtido no encerramento dessa etapa de disputa.

3.4.4. O estímulo contínuo da disputa de preços no modo aberto, ou seja, os lances sucessivos e públicos, afasta todo risco de empresas amadoras (novas no mercado) lançarem valor fora do mercado numa etapa fechada (que é sigilosa). Os preços em disputa aberta ficam claros para melhor competição entre os participantes. Então, evitar riscos na contratação contribui para ter uma licitação que alcance mais prontamente os resultados pretendidos.

3.4.5. Outrossim, não foi possível identificar que optar por modo disputa diferente do "modo aberto" venha a trazer vantagem para a Administração e nem mesmo aponta simplificação do processo ou celeridade no resultado da licitação.

3.5. **Da Vigência Contratual:**

3.5.1. O prazo de vigência da contratação é de **até 60 (sessenta) meses**, contados da assinatura do instrumento contratual, pelas partes, com execução a partir do recebimento da primeira Ordem de Serviço, com prorrogação, na forma do artigo 106 ou 107, da Lei n° 14.133, de 2021.

3.5.2. A contratação terá eficácia, **a contar da assinatura do contrato**, com fulcro no artigo **94, Inciso I** da lei de licitações 14.133/2021.

3.5.3. Encerrado o procedimento licitatório, o representante legal da empresa cuja proposta foi declarada vencedora será convocado via sistema eletrônico e e-mail para firmar/assinar o Contrato ou instrumento equivalente.

3.5.4. Será facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

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

3.5.6. Por ter sido adotado a modalidade de Pregão Eletrônico, com julgamento de Menor Preço por Global, a contratação posterior de item específico constante de grupo de itens, exigirá prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou entidade , conforme está previsto no § 2º, art. 82, da Lei 14.133 de 2021.

3.5.7. A justificativa detalhada conforme o item 5.12. Estudo Técnico Preliminar 47 (70175357)

O prazo de vigência da contratação é de 60 (sessenta) meses, conforme vier a constar do(s) contrato(s) ou instrumento substituto (se for o caso).

O prazo estipulado garante a continuidade operacional dos serviços de TIC, evitando descontinuidade, interrupções e custos decorrentes de contratações frequentes. A continuidade é fundamental para a estabilidade dos serviços, a segurança da informação, a satisfação dos usuários e o cumprimento das metas institucionais. Ainda, também permite o planejamento de longo prazo, a integração de novos projetos e a adaptação a mudanças tecnológicas e regulatórias.

A amortização dos investimentos em equipamentos ao longo de 60 meses otimiza o uso dos recursos públicos, diluindo os custos de aquisição, instalação, integração, treinamento e manutenção ao longo do tempo. Essa abordagem evita ociosidade de ativos, desperdício de recursos e necessidade de aquisições emergenciais, promovendo a eficiência e a sustentabilidade financeira da instituição.

O prazo de 60 meses está alinhado ao ciclo de vida útil dos equipamentos, conforme especificações técnicas, recomendações dos fabricantes e práticas de mercado. O ciclo de vida útil dos equipamentos de TIC geralmente varia entre 48 e 72 meses, dependendo do tipo de equipamento, da intensidade de uso, das condições ambientais e das políticas de atualização tecnológica. O prazo de 60 meses garante que os ativos permaneçam atualizados, operacionais e em conformidade com os requisitos de desempenho e segurança durante todo o período contratual.

O período de vigência coincide com a garantia estendida dos equipamentos, assegurando cobertura para manutenção corretiva e preventiva, substituição de peças, atualização de software e suporte técnico, conforme exigido no ETP. A garantia estendida reduz os riscos de indisponibilidade, falhas e custos adicionais de manutenção, promovendo a confiabilidade e a disponibilidade dos serviços de TIC.

O prazo de 60 meses facilita o planejamento orçamentário, a previsibilidade de despesas, a gestão de contratos e a prestação de contas, em conformidade com as exigências da Lei de Responsabilidade Fiscal (Lei Complementar nº 101/2000) e das normativas de governança de TIC. O planejamento de longo prazo permite a alocação eficiente de recursos, a negociação de condições comerciais vantajosas e a adaptação a mudanças no ambiente institucional.

Além disso, o prazo de 60 meses está alinhado às diretrizes de sustentabilidade ambiental, ao evitar o descarte prematuro de equipamentos, promover a reutilização, a reciclagem e a destinação adequada de resíduos, em conformidade com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010) e o Decreto nº 10.940/2022.

Portanto, o prazo de 60 meses é justificado por critérios de continuidade, eficiência, sustentabilidade, governança, planejamento orçamentário, ciclo de vida dos equipamentos e alinhamento com as melhores práticas de gestão pública, promovendo a excelência na contratação de bens e serviços de TIC.

3.6. **Da vigência da ata de registro de preços (Art. 42, § 1º, IV, Dec. Estadual nº 28.874/2024):**

3.6.1. O prazo de vigência da ata de registro de preços, contado a partir da publicação do extrato da ata na imprensa oficial, será de 12 (doze) meses, e poderá ser prorrogado, por igual período, desde que comprovado que as condições e o preço permanecem vantajosos, conforme **art. 125**, do Decreto Estadual nº 28.874/2024.

3.6.2. No ato de prorrogação da vigência da ata de registro de preços poderá haver a renovação dos quantitativos registrados, até o limite do quantitativo original.

3.6.3. O ato de prorrogação da vigência da ata deverá indicar expressamente o prazo de prorrogação e o quantitativo renovado

3.7. **Contratações Correlatas e Resultados Pretendidos:**

3.7.1. Não contratações correlatas, conforme disposição constante do item 14. do Estudo Técnico Preliminar 47 (70175357)

3.8. **Risco:**

3.8.1. A Mapa de Risco 220 (0057454896).

3.9. **Das Quantidades Estimadas para a Contração:**

3.9.1. A definição das quantidades de equipamentos a serem contratados é resultado de um processo rigoroso de levantamento de necessidades, dimensionamento técnico, análise de mercado, avaliação do histórico de contratações similares e projeção de demanda futura, conforme preconizam as principais normativas do setor público, especialmente a Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos), a Instrução Normativa SEGES nº 58/2022, a Instrução Normativa SGD/ME nº 94/2022 e o Decreto nº 28.874/2024.

3.9.2. A métrica adotada baseia-se na capacidade de atendimento das demandas atuais e futuras da infraestrutura tecnológica da SEDUC-RO, considerando o volume de tráfego de dados, número de conexões simultâneas, requisitos de alta disponibilidade, e resiliência contra ameaças cibernéticas. A solução escolhida contempla dois appliances em cluster, com capacidade mínima de 60 Gbps em camada 7 e 95 Gbps em camada 4, refletindo a necessidade de suportar o tráfego de aplicações críticas em todas as unidades escolares e administrativas integradas aos Data Centers Principal e Backup.

3.9.3. Assim, o quantitativo ora proposto foi definido conforme descrito na Informação 14 - Memória de Cálculo (67571362), e todos os quantitativos previstos foram definidos com base em critérios técnicos adequados e financeiramente racionais, respeitando o planejamento orçamentário vigente, bem como os objetivos operacionais da SEDUC/RO. A proposta atende integralmente aos princípios da eficiência, economicidade e continuidade na prestação dos serviços de Tecnologia da Informação e Comunicação(TIC).

Tabela A-1

ESTIMATIVA DAS QUANTIDADES								
Item	**Cód. Catálogo CATMAT/CATSERV**	**Objeto**	**Detalhamento do Objeto**	**Categoria**	**Quantidade Aplicada**	**Quantidade**	**Valor unidade R$**	**Valor Total R$**
1	481646	Solução de Firewall de Aplicação Web (Web Application Firewall)	Solução de Firewall de Aplicação Web - WAF configurados em cluster de 2 hardwares.	Hardware	2 - Datacenter **A** (PRM) 2 - Datacenter **B** (DR)	4	R$ 2.949.336,90	R$ 11.797.347,60
2	27090	Licenciamento e garantia da Solução de Firewall de Aplicação Web (Web Application Firewall)	Licenças de uso dos softwares de gerenciamento da solução, junto com a garantia dos mesmos.	Licença de uso	2 - Datacenter **A** (PRM) 2 - Datacenter **B** (DR)	4	R$ 2.373.132,14	R$ 9.492.528,56
3	27111	Serviço de instalação e configuração da Solução de firewall de aplicação Web.	Serviços de instalação, transição e configuração / parametrização dos equipamentos e softwares da Solução de firewall de aplicação Web - WAF.	Serviço	2 - Datacenter **A** (PRM) 2 - Datacenter **B** (DR)	4	R$ 45.431,42	R$ 181.725,68
4	27014	Manutenção e suporte da Solução de Firewall de Aplicação Web (Web Application Firewall).	Serviços de suporte assistido, com manutenções a infraestrutura dos equipamentos e softwares.	Serviço	60 - Meses de suporte as soluções	60	R$ 34.774,11	R$ 2.086.446,60
5	16837	Treinamento do fabricante da solução para (10 participantes).	Serviços de treinamento das soluções (POR SOLUÇÃO).	Serviço	Serviços de treinamento das soluções (Por Participante).	10	R$ 7.459,10	R$ 74.591,00
6	26077	Solução de Segurança Avançada	Solução de Segurança Avançada, proteção uniforme e consistente às aplicações expostas à Internet (a cada 20 FQDNs).	Serviço	Licenciamento para 20 FQDNs	4	R$ X.XXX,XX	R$ X.XXXX,XX
							Total	**R$ 23.632.639,44**

3.9.4. Segue a relação de processos de aquisições de dispositivos fora de garantia, que serão substituídos com a contratação:

Tabela A-2

Processo de Aquisição	**Quadro de Distribuição**	**Dados de Contrato**	**Tipo de dispositivo**	**Quantidade**
0029.135533/2020-45	Servidores Físicos: 04	Contrato N° 298/PGE-2020 (0012422213)	Firewall de Aplicação WEB - WAF Datacenter A + B(DR)	4
Total de Dispositivos				4

3.9.5. Ademais, há justificativa nos autos quanto a estimativa das quantidades, conforme Despacho 0061657947 emitido pela Gerência de Segurança da Informação e Operação de Redes - GSIOR.

A definição das quantidades de equipamentos a serem contratados é resultado de um processo rigoroso de levantamento de necessidades, dimensionamento técnico, análise de mercado, avaliação do histórico de contratações similares e projeção de demanda futura, conforme preconizam as principais normativas do setor público, especialmente a Lei nº 14.133/2021 (Nova Lei de Licitações e Contratos Administrativos), a Instrução Normativa SEGES nº 58/2022, a Instrução Normativa SGD/ME nº 94/2022 e o Decreto nº 28.874/2024.

O levantamento de necessidades foi realizado a partir de um diagnóstico institucional detalhado, envolvendo análise com gestores e processos de trabalho, inventário de ativos de TIC e identificação de gargalos operacionais. Esse diagnóstico permitiu mapear os setores, unidades e perfis de usuários que demandam os equipamentos, considerando não apenas o cenário atual, mas também as projeções de crescimento institucional, expansão de serviços e adoção de novas tecnologias previstas no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). O levantamento foi documentado no Estudo Técnico Preliminar (ETP), em conformidade com o art. 18 da Lei nº 14.133/2021, que exige a adequada caracterização do objeto e a demonstração da necessidade da contratação.

As informações referentes aos quantitativos dos itens a serem adquiridos com vistas à contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações Web da SEDUC-RO, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização.

A métrica adotada baseia-se na capacidade de atendimento das demandas atuais e futuras da infraestrutura tecnológica da SEDUC-RO, considerando o volume de tráfego de dados, número de conexões simultâneas, requisitos de alta disponibilidade, e resiliência contra ameaças cibernéticas. A solução escolhida contempla dois appliances em cluster, com capacidade mínima de 60 Gbps em camada 7 e 95 Gbps em camada 4, refletindo a necessidade de suportar o tráfego de aplicações críticas em todas as unidades escolares e administrativas integradas aos Data Centers Principal e Backup.

Os dispositivos e licenças contemplados foram mapeados com base na contratação anterior realizada por meio do **Processo SEI nº** 0029.135533/2020-45 (Modalidade: Adesão à Ata de Registro de Preços – Participante).

Assim, o quantitativo ora proposto foi definido conforme descrito na Informação 3 - Memória de Cálculo (0062762071), e todos os quantitativos previstos foram definidos com base em critérios técnicos adequados e financeiramente racionais, respeitando o planejamento orçamentário vigente, bem como os objetivos operacionais da SEDUC/RO. A proposta atende integralmente aos princípios da eficiência, economicidade e continuidade na prestação dos serviços de Tecnologia da Informação e Comunicação(TIC).

O dimensionamento técnico dos equipamentos considerou critérios de desempenho, capacidade, compatibilidade, escalabilidade e sustentabilidade, alinhados às melhores práticas de gestão de ativos de TIC, como ITIL e COBIT. Foram avaliados requisitos mínimos e recomendados para cada tipo de equipamento, levando em conta a criticidade das atividades suportadas, a necessidade de alta disponibilidade, a interoperabilidade com sistemas legados e a aderência às políticas de segurança da informação. O dimensionamento também contemplou a necessidade de reserva técnica para atendimento a emergências, substituição de equipamentos defeituosos e suporte a projetos estratégicos.

A análise de mercado foi conduzida por meio de pesquisa de preços, especificações técnicas e condições comerciais junto a fornecedores qualificados, observando padrões de mercado, ciclos de atualização tecnológica, disponibilidade de peças e serviços de manutenção, bem como práticas sustentáveis de produção e descarte. Essa análise permitiu identificar tendências de mercado, inovações tecnológicas, oportunidades de economia de escala e riscos de desabastecimento, conforme orienta o art. 23 da IN SGD/ME nº 94/2022. Também foram consideradas as diretrizes de sustentabilidade ambiental, em consonância com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010) e o Decreto nº 10.940/2022, priorizando equipamentos com certificações ambientais, baixo consumo energético e facilidade de reciclagem.

O histórico de contratações similares foi analisado a partir de registros de contratos anteriores, relatórios de utilização, índices de substituição, obsolescência e eventuais sobras ou faltas de equipamentos. Essa avaliação permitiu ajustar a previsão de aquisição, evitando tanto a insuficiência quanto o excesso de equipamentos, promovendo a economicidade e a eficiência do gasto público, em conformidade com o princípio da eficiência previsto no art. 5º da Lei nº 14.133/2021. Foram identificados padrões de uso, ciclos de vida útil, taxas de falha e necessidades de atualização, subsidiando a definição de quantitativos realistas e aderentes à demanda institucional.

A projeção de demanda futura considerou fatores como crescimento estimado de usuários, expansão de serviços, adoção de novas tecnologias, necessidade de reposição por obsolescência e falhas, bem como a reserva técnica para atendimento a emergências e continuidade operacional. Foram utilizados modelos de previsão baseados em séries históricas, análise de tendências e benchmarking com instituições similares, garantindo a robustez das estimativas e a aderência às melhores práticas de planejamento de TIC.

Dessa forma, as quantidades propostas refletem o equilíbrio entre a suficiência para atendimento das demandas institucionais e a observância do princípio da economicidade, evitando aquisições desnecessárias e promovendo o uso racional dos recursos públicos. A metodologia adotada assegura a transparência, a rastreabilidade e a justificativa técnica das decisões, em conformidade com as exigências legais e normativas aplicáveis.

3.9.6. As quantidades e seus detalhamentos, foram apresentadas com base nas informações enviadas pela Coordenadoria de Tecnologia da Informação e Comunicação (COTIC), por meio do Memorando nº 56/2024/SEDUC-GSIOR (0056845723), e do Formulário Levantamento de Necessidades (0056680903), nos autos do Processo 0029.067555/2024-07.

3.9.7. Dessa forma, os produtos devem ser adquiridos levando em consideração as quantidades abaixo, bem como as características descritas neste estudo.

GRUPO	Classe (CATMAT / CATSER)	Item	Detalhamento do Objeto	Unidade de Medida	Quantidade
1	481646	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com garantia para 60 meses.	Unidade	4
	27090	2	Licenciamento e garantia da Solução de Firewall de Aplicação Web (Web Application Firewall) com garantia e suporte para 60 meses.	Unidade	4
	27111	3	Serviço de instalação e configuração da Solução de firewall de aplicação Web.	Unidade	4
	27014	4	Manutenção e suporte da Solução de Firewall de Aplicação Web (Web Application Firewall).	Mês	60
	16837	5	Treinamento na solução para (10 participantes).	UNIDADE	10
	26077	6	Solução de Segurança Avançada, com garantia para 60 meses	Unidade	4

4. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO:

4.1. Descrição da Necessidade da Contratação:

4.1.1. O ambiente educacional depende fortemente de soluções tecnológicas para assegurar a continuidade e a eficiência das atividades acadêmicas e administrativas. Atualmente, todas as unidades escolares e administrativas conectadas ao Data Center da SEDUC, localizado na sede administrativa (CPA), utilizam a rede IP/MPLS e a rede INFOVIA do Governo do Estado de Rondônia. Essas redes são fundamentais para o acesso aos sistemas informatizados da Secretaria e para a comunicação via internet, garantindo a operacionalidade e a qualidade dos serviços educacionais prestados à população.

4.1.2. No entanto, os equipamentos atualmente em operação, adquiridos por meio do Processo SEI nº 0029.135533/2020-45, CONTRATO N° 299/PGE-2020 (0012423252), encontram-se com contratos de garantia e suporte expirados, impossibilitando a renovação mediante simples aditamento, conforme as especificações contratuais do fabricante. Além disso, esses equipamentos não mais atendem às demandas tecnológicas atuais, colocando em risco a segurança e a eficiência da infraestrutura de TI da SEDUC.

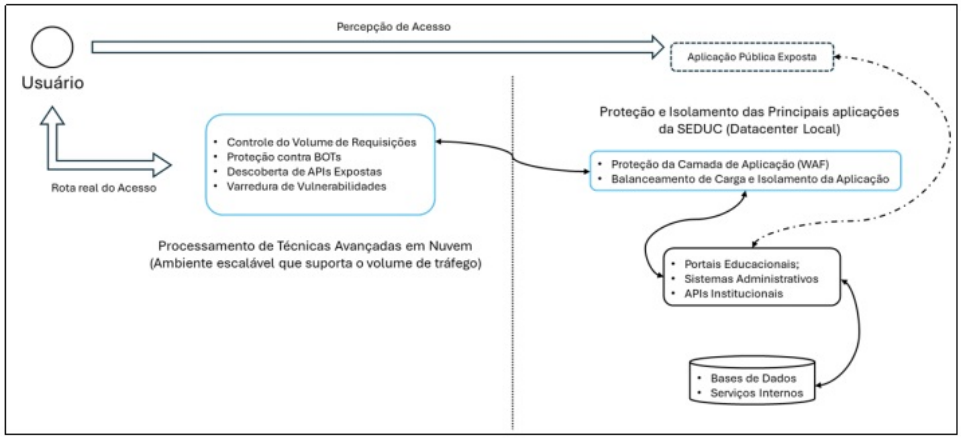
4.1.3. Nos últimos anos, ataques cibernéticos direcionados a órgãos públicos e entidades governamentais tornaram-se cada vez mais frequentes e sofisticados. Em 2023, o Brasil registrou diversos incidentes relevantes que evidenciam a vulnerabilidade de instituições públicas. Casos como o ataque ao Supremo Tribunal Federal (STF) e ao Ministério da Saúde em anos anteriores, bem como incidentes recentes envolvendo sistemas de universidades e instituições estaduais, demonstram o impacto significativo que falhas de segurança podem causar.

4.1.4. Esses ataques, frequentemente baseados em ransomware, phishing direcionado e exploração de vulnerabilidades em aplicações web, resultam em paralisações de serviços, vazamento de dados sensíveis e prejuízos financeiros significativos. Relatórios recentes de empresas de segurança indicam que a área da educação está entre os setores mais visados por cibercriminosos devido à grande quantidade de dados armazenados e ao acesso remoto amplamente utilizado por servidores e alunos.

4.1.5. Diante desse cenário, a adoção de um Firewall de Aplicação Web (WAF) é imprescindível para a SEDUC-RO, pelos seguintes motivos:

- Proteção Contra Ameaças Cibernéticas – Um WAF permite identificar e mitigar ataques avançados, protegendo aplicações web contra ameaças como injeção de SQL, cross-site scripting (XSS) e exploração de vulnerabilidades.
- Garantia da Continuidade dos Serviços Educacionais – A segurança das aplicações web é fundamental para assegurar o acesso ininterrupto aos sistemas educacionais e administrativos, impactando diretamente na qualidade dos serviços oferecidos à população.
- Conformidade com Normas de Segurança – A contratação de soluções modernas está alinhada à Política de Segurança da Informação (PSI), instituída pela Portaria nº 97, de 09 de junho de 2021, da SETIC/RO, que estabelece os princípios de integridade, confidencialidade, autenticidade e disponibilidade.
- Prevenção de Danos Financeiros e Reputacionais – Incidentes de segurança podem comprometer a prestação de serviços essenciais, além de gerar prejuízos financeiros e impactar negativamente a imagem da instituição.
- Elevação da Postura de Segurança – A implementação de uma solução WAF robusta fortalecerá a segurança da informação da SEDUC-RO, protegendo seus ativos críticos e garantindo a continuidade das operações.

4.1.6. O aumento do volume de acessos, a ampliação do número de aplicações expostas à Internet e a sofisticação das ameaças cibernéticas demandam mecanismos adicionais de proteção, capazes de assegurar disponibilidade, desempenho e integridade das aplicações institucionais, tais como portais educacionais, sistemas de matrícula on-line, gestão acadêmica e plataformas de ensino remoto. A adoção da Plataforma de Segurança Avançada complementa a camada de proteção on-premise, ampliando a capacidade de mitigação de ataques, prevenção de indisponibilidades e resposta a incidentes, de forma integrada, escalável e alinhada às boas práticas de segurança da informação, garantindo a continuidade dos serviços essenciais prestados pela SEDUC-RO.



4.1.7. A imagem acima ilustra a arquitetura pretendida com a contratação, bem como exemplifica o nível de transparência – quanto a percepção qualitativa do usuário; no acesso seguro, controlado e preventivo (na mitigação de ataques cibernéticos), o qual a SEDUC-RO almeja adotar com a contratação a ser vigorada.

4.1.8. Nesse contexto, o investimento em uma solução de balanceamento de carga e Web Application Firewall (WAF), representa um pilar estratégico para assegurar a continuidade dos serviços, reduzir indisponibilidades e proteger aplicações críticas contra falhas e ataques, preservando a qualidade do atendimento público e a confiança dos cidadãos.

4.1.9. Do ponto de vista técnico-operacional, a capacidade complementar da solução em balancear as sessões de comunicação, permite a distribuição eficiente do tráfego entre múltiplos servidores, garantindo alta disponibilidade, escalabilidade e melhor utilização dos recursos existentes no datacenter estadual.

4.1.10. Associado a um WAF, esse modelo fortalece a segurança na borda da infraestrutura, mitigando ameaças comuns como injeção de código, cross-site scripting e exploração de vulnerabilidades conhecidas, além de atender a requisitos de governança, controle e soberania dos dados, fundamentais para a administração pública.

4.1.11. Tal investimento contribui diretamente para o incremento da maturidade técnica da Secretaria, reduzindo riscos operacionais e dependências excessivas de intervenções manuais.

4.1.12. Complementarmente, a adoção de uma arquitetura fim-a-fim, integrada a uma solução de Segurança Avançada hospedada na nuvem, amplia significativamente o nível de proteção e inteligência da plataforma.

4.1.13. Essa camada adicional possibilita a aplicação de controles modernos, como a limitação e a modelagem do volume de requisições às aplicações, a proteção contra bots maliciosos e automatizados, bem como a identificação de padrões anômalos de acesso.

4.1.14. Por conseguinte, recursos de descoberta de APIs indevidamente expostas e a varredura contínua de vulnerabilidades na camada de aplicação permitem uma postura proativa de segurança, antecipando riscos que dificilmente seriam detectados apenas com mecanismos tradicionais locais.

4.1.15. Por fim, a combinação entre soluções e serviços avançados estabelece um equilíbrio entre controle, desempenho e inovação, alinhado às melhores práticas de arquitetura híbrida adotadas no setor público.

4.1.16. Essa estratégia não apenas eleva o nível de segurança cibernética da Secretaria de Estado da Educação de Rondônia, como também promove a evolução técnica de suas equipes, ao incorporar processos e tecnologias modernas de proteção de aplicações.

4.1.17. O resultado é um ambiente mais resiliente, seguro e preparado para sustentar a expansão dos serviços digitais educacionais, beneficiando diretamente a população e fortalecendo a capacidade institucional do Estado.

4.1.18. Portanto, torna-se imperativo que a SEDUC-RO realize a contratação de uma empresa especializada para o fornecimento de uma solução de Firewall de Aplicação Web (WA F). Essa contratação é essencial para garantir a proteção das aplicações web, salvaguardar informações sensíveis e assegurar a continuidade dos serviços educacionais prestados pelo Governo do Estado de Rondônia.

4.2. **Justificativa do Parcelamento ou Não da Contratação**

4.2.1. Sobre essa questão, a Súmula no 247 do TCU estabeleceu o seguinte:

> "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade".

4.2.2. Outrora esse entendimento, consideramos que não é possível afirmar sumariamente, sem a análise do caso concreto, que a licitação por itens ou por lote único seria mais eficiente. O próprio TCU já teve a oportunidade de se manifestar no sentido de que, no caso específico, a licitação por lote único seria a mais eficiente à administração:

> "Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços ... Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão no 3140/2006 do TCU)."

4.2.3. Nos termos do art. 47, inciso II, da Lei Federal nº 14.133/2021, as licitações atenderão ao princípio do parcelamento, quando tecnicamente viável e economicamente vantajoso.

4.2.4. Em via de regra, as aquisições da Administração Pública devem atender ao princípio do parcelamento, que deverá ser adotado quando for tecnicamente viável e economicamente vantajoso, conforme artigo 40, inciso V, alínea b, da Lei nº 14.133/2021. Vejamos:

> *Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:*
>
> *(...)*
>
> *V - atendimento aos princípios:*
>
> *a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;*
>
> *b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso;*
>
> *c) da responsabilidade fiscal, mediante a comparação da despesa estimada com a prevista no orçamento.*
>
> [...]
>
> § 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:
>
> I - a viabilidade da divisão do objeto em lotes;
>
> II - o aproveitamento das peculiaridades do mercado local, com vistas à economicidade, sempre que possível, desde que atendidos os parâmetros de qualidade; e
>
> III - o dever de buscar a ampliação da competição e de evitar a concentração de mercado.
>
> Contudo, conforme descrito no §3º do dispositivo citado, o parcelamento não será adotado nas seguintes situações:
>
> § 3º O parcelamento não será adotado quando:
>
> I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;
>
> II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;
>
> III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.

4.2.5. A licitação em grupo consiste na reunião de itens em um mesmo lote, de modo que a disputa ocorra de forma global, resultando na contratação de um único fornecedor para o provimento do conjunto da solução. Do ponto de vista técnico, todos os itens da pretensão contratual fazem parte de uma solução integrada, de modo que sua divisão seria prejudicial ao conjunto do objeto.

4.2.6. Embora a solução seja, em tese, divisível, há interesse técnico na manutenção da unicidade. Não se trata apenas da aplicação da regra geral que dirige o processo decisório, mas sim da sua viabilidade técnica.

4.2.7. Dessa forma, a avaliação sob o aspecto técnico precede a avaliação econômica, pois não se trata de contratar uma solução pelo menor preço simplesmente. Em nossa avaliação, a manutenção da unicidade (indivisibilidade) garante os benefícios da solução, sendo conveniente à Administração que assim seja licitado.

4.2.8. Os serviços objeto da contratação, bem como os insumos apresentados, são correlatos e devem ser geridos e executados pela mesma empresa. Caso contrário, poderia haver uma demanda complexa e desnecessária para os fiscais contratuais, resultando em serviços com padrões de qualidade inconsistentes e ingerência entre diferentes empresas, se o objeto fosse dividido em lotes independentes.

4.3. **Do Agrupamento dos Itens por Lote:**

4.3.1. O objeto do presente Termo de Referência é a "Contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software **",** visando a manutenção da atual rede da SEDUC-RO, conforme condições e exigências, constantes deste instrumento, à luz da Lei Geral de Licitações e da Súmula nº. 8/TCE-RO, de maneira que a fragmentação em itens **acarretaria a perda do conjunto; perda da econômica de escala; redundaria em prejuízo à celeridade da licitação; ocasionaria a excessiva pulverização de contratos ou resultaria em contratos de pequena expressão econômica.**

4.3.2. Segundo o Doutor Marçal Justen Filho, o fracionamento [1]*"respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável"*

4.4. **Do agrupamento por lote de itens que guardem homogeneidade entre si:**

4.4.1. Nas licitações de objetos divisíveis o Tribunal de Contas da União entende que o julgamento seja feito por item, e não por preço por lote. Contudo, há situações em que se faz necessário aglutinar os itens com o intento de casar aquisições, visto que poderá haver um vínculo entre eles, ou se comprados separadamente prejudicarão o resultado esperado pela Administração.

4.4.2. Nesse caso, apesar dos objetos serem divisíveis, eles guardam estrita identidade de natureza e características semelhantes, além de guardar correspondência com sua composição, podendo serem executados por um mesmo prestador de serviços, por se tratarem de objetos comuns ao ramo de *serviços de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software"***,** visando a manutenção da atual rede da SEDUC-RO, concretizando, assim, os princípios da competitividade.

4.5. **Da fragmentação em itens acarretar a perda do conjunto:**

4.5.1. O parcelamento do objeto somente se justifica e fundamenta quando houver viabilidade técnica e, principalmente, ganho econômico para a Administração Pública. No presente caso não há viabilidade técnica, uma vez que a falta de um tipo de serviço prejudicaria todo o conjunto, e, de nada adiantaria ter por tratar-se de um conjunto de soluções que precisam trabalhar de forma integrada para garantir sua eficiência e compatibilidade. Ter uma gerência integrada diminui a curva do aprendizado e possibilita sua gestão com poucos colaboradores especializados o que não aconteceria caso fosse adjudicação por item.

4.5.2. Em se tratando de "Contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software**",** visando a manutenção da atual rede da SEDUC-RO, conforme condições e exigências, constantes deste instrumento, não podemos considerar o fator econômico como preponderante, mas mesmo assim entendemos que a adjudicação por lote, dentro da economia de escala, também possibilitará um desembolso menor dos cofres públicos do que se todos os itens fossem adquiridos de forma distinta. Podemos acrescentar também, caso a adjudicação fosse por item, quanto a dificuldade de gestão dos contratos de suporte e de sua eficiência, além da possibilidade de conflito na utilização dos recursos e sua complexidade, como por exemplo. Há necessidade que todos os itens estejam disponíveis para a adequada utilização de todos equipamentos.

4.6. **Da perda da economia de escala:**

4.6.1. As compras efetuadas pela Administração devem ser divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

4.6.2. Quanto maior a quantidade a ser executada, maior poderá ser o desconto na contratação de serviços. Esse ganho está relacionado com o aumento da quantidade adquirida sem um aumento proporcional no custo e está intrinsicamente relacionado ao princípio da economicidade esculpido no art. 70 de nossa Carta Magna.

4.6.3. A economia de escala é definida como aquela que ocorre a partir de determinado patamar de quantidade de itens comercializados e pode acarretar relevante desconto na aquisição dos bens e serviços.

4.6.4. De tal modo, que no caso em tela a adoção critério de julgamento menor preço permite o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade, sem perda da economia de escala, como por exemplo, a empresa que ganhar o lote fornecerá todos os itens, acarretando, consequentemente, uma diminuição nos custos e economia de escala.

4.7. **Do prejuízo à celeridade da licitação:**

4.7.1. Um dos fatores que pode ser levado em conta na elaboração de um edital por lote é o interesse na celeridade do processo.

4.7.2. Neste caso, trata-se de 01 (um) Lotes, com quantidades distintas de itens. Assim, a "Contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software **",** visando a manutenção da atual rede da SEDUC-RO, conforme condições e exigências, constantes deste instrumento, conjuntamente, por uma única empresa por lote, fica mais célere o julgamento das propostas. Caso contrário, seriam estabelecidos vários prazos entre várias empresas para conclusão do objeto contratado, e com isso, poderia haver um grande embaraço.

4.8. **Da pulverização de contratos:**

4.8.1. A licitação por itens corresponde, na verdade, a uma multiplicidade de licitações, cada qual com existência própria e dotada de autonomia jurídica, mas todas desenvolvidas conjugadamente em um único procedimento, documentado nos mesmos autos. Esta exagerada divisão de objeto pode ocasionar uma excessiva pulverização dos contratos, tornando mais dispendiosa a contratação.

4.8.2. No caso em questão, a adoção do critério de julgamento menor preço por lote para a "Contratação de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software **",** visando a manutenção da atual rede da SEDUC-RO, conforme condições e exigências, constantes deste instrumento, resultaria na contratação de 1 (uma) única empresas fornecedora/licitantes por lote, não ocorrendo a pulverização de contratos. Ainda há, com base no interesse público, maior segurança ao cumprimento do contrato.

4.8.3. Por fim, há que se observar o caso concreto, avaliando a conveniência e oportunidade, de modo a satisfazer da melhor forma o interesse público, pois cada contratação tem suas especificidades, in casu a aquisição por lote é mais vantajosa para a Administração, em decorrência dos riscos inerentes à própria execução, pois, não restam dúvidas, o objeto pretendido, quando executado por vários contratados, poderá não ser integralmente entregue, tendo em vista problemas na relações jurídicas mantidas com diversos contratados.

4.9. **Levantamento de Mercado:**

4.9.1. O levantamento mercado consiste na análise das alternativas possíveis, bem como a justificativa técnica e econômica da escolha do tipo de solução a contratar (art. 18, §1º, V da Lei 14.133/2021).

4.9.2. A seguir, são apresentadas algumas opções de soluções integradas disponíveis no mercado:

- **SOLUÇÃO 01: Aquisição de conjunto de equipamentos de forma separada**

4.9.2.1. Solução composta por um conjunto de equipamentos, *appliances*, que tratam, cada um, de uma funcionalidade específica. Neste caso a solução nunca será composta apenas por um equipamento e, portanto, apresentará maiores dificuldades de gerenciamento das funcionalidades, pois cada equipamento terá sua plataforma de gerência.

PONTOS POSITIVOS	PONTOS NEGATIVOS
a) Estrutura da solução mais robusta; b) Apresenta a possibilidade de aquisição de appliance dedicado para apenas uma funcionalidade considerada essencial para estruturar ou adicionar a infraestrutura de rede existente, e que necessite maior robustez; e c) Podem ser contratadas separadamente conforme a necessidade da SEDUC	a) Exige gerenciamento descentralizado das soluções, pois cada appliance apresenta sua plataforma própria de gerência; b) Necessita de equipe técnica maior e mais capacitada para operacionalização dos equipamentos; c) O custo de soluções segregadas geralmente é maior que as integradas; d) Dificuldade para correlacionar e analisar eventos em plataformas distintas o que impacta no poder e na tempestividade da reação do órgão diante de incidentes de segurança; e) Ocupam mais espaço no Data Center e apresentam maior consumo de energia.

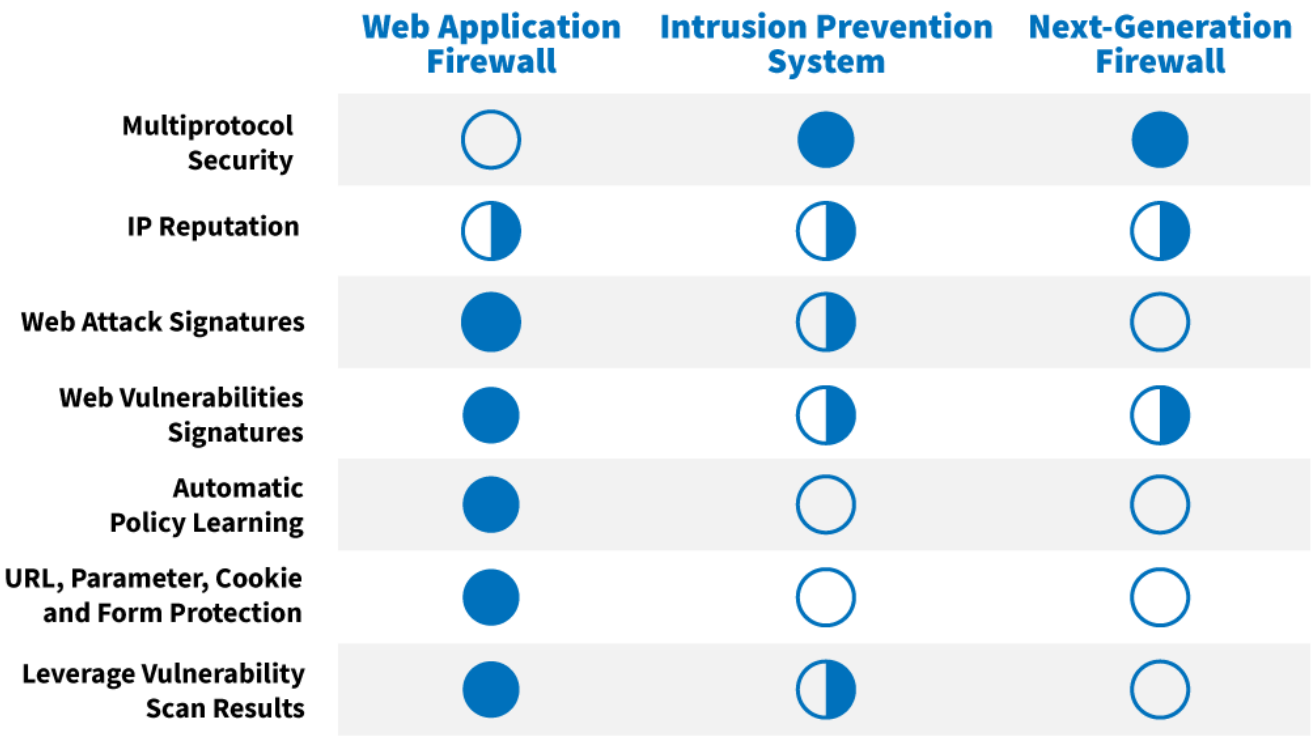
4.9.2.2. A aquisição de equipamentos específicos para cada funcionalidade (balanceamento, filtro de pacotes, anti-malware, VPN, filtro de camada de aplicação, entre outros, não é uma solução muito eficiente, pois dificultará o gerenciamento e correlação dos eventos de segurança, característica relevante das soluções mais integradas, o que pode dificultar a detecção, contenção e o tratamento de uma incidente de segurança, elevando o risco de vazamento de dados e indisponibilidade dos serviços. Além disso, exigirá muitos especialistas com conhecimento nos diversos equipamentos ou soluções adquiridas e apresentará mais curto de espaço e energia.

4.9.2.3. Logo, não se mostra uma solução viável aos interesses da SEDUC/RO.

- **SOLUÇÃO 02: Aquisição de equipamento do tipo NGFW – Firewall Corporativo com a funcionalidade de firewall de aplicação web (WAF)**

4.9.2.4. Nessa solução a funcionalidade de firewall de aplicações web ou proteção contra ataques de camada de aplicação é realizado pelo firewall de próxima geração e a topologia da borda é composta por dois clusters deste tipo de equipamento. O NGFW constitui-se de equipamento capaz de agregar as diversas funcionalidades de segurança entre Firewall, Antivírus, IDS /IPS, WebFilter e outros, apresentando co-relacionamento de dados entre os resultados das diversas funcionalidades. Estes equipamentos podem realizar inspeção em camada de aplicação e utilizam a mesma plataforma de gerência para todas as funcionalidades. Porém a inspeção realizada da camada de aplicação não é comparável ao nível de granularidade de inspeção de um equipamento WAF dedicado que ainda disporá de balanceamento de carga e DNS. Em muitas situações, para contar nos NGFW com essa capacidade de inspeção do tráfego na camada de aplicação, faz-se necessário contratar licenciamento adicional para seu uso. O WAF dedicado garantirá maior capacidade de inspeção e análise dos pacotes de camada 7 evitando uma maior latência e desonerando o NGFW para outras análises, garantindo melhor thoughput da rede.

4.9.2.5. Vejamos as principais diferenças entre o WAF, IPS e NGFW:



4.9.2.6. A análise da Xlabs Security (https://www.xlabs.com.br/) da figura acima, demonstra que o WAF dedicado tem atuação melhor comparada ao NGFW e ao IPS no que refere-se a assinaturas de vulnerabilidades web, aprendizado automático de políticas, proteção granular de URLs (Universal Resource Location), parâmetros, cookies e formulários das aplicações e melhor resultado médio em busca de vulnerabilidades.

4.9.2.7. Pelo exposto, essa solução não é viável para o atendimento às necessidades de segurança cibernética da SEDUC.

4.9.2.8. A solução consiste em uma plataforma dedicada de Firewall de Aplicações Web (WAF), integrada a funções de Balanceamento de Carga (ADC) e gerenciamento de DNS. Diferente de firewalls de rede genéricos, este equipamento é projetado especificamente para a inspeção profunda e granular da Camada de Aplicação, permitindo a correlação de dados e eventos em tempo real sob uma gestão unificada. A solução deve garantir a mitigação de ataques complexos, a aceleração de tráfego e a alta disponibilidade dos serviços, provendo um nível de visibilidade e controle superior às inspeções superficiais de firewalls convencionais.

PONTOS POSITIVOS	PONTOS NEGATIVOS
a) É uma evolução da já consolidada plataforma unificada do tipo UTM sendo, inclusive, muitas fornecidas pelos mesmos fornecedores de UTM; b) Plataforma de gerenciamento unificado para as diversas funcionalidades de segurança de redes; c) Possuem garantia de capacidade para análise do tráfego por funcionalidade; d) Apresentam o maior nível de visibilidade no monitoramento e controle de ameaças devido ao correlacionamento das informações provenientes das diferentes funcionalidades; e) Exige menor conhecimento técnico/operacional por parte da equipe uma vez que as ferramentas de gerenciamento já são mais intuitivas e direcionadas para a configuração dos principais cenários de segurança de redes; f) Apresentam praticamente todas as funcionalidades essenciais à estruturação de uma solução de segurança de redes computacionais; g) Apresentam, adicionalmente, a capacidade de detectar malwares e ameaças em um nível satisfatório; h) Podem ser adquiridas em diversos portes de capacidade conforme a capacidade da SEDUC, resultando em formas mais eficientes de utilização dos recursos do equipamento e no custo de aquisição.	a) Podem gerar problemas no dimensionamento de capacidade da appliance uma vez que sua performance depende de quais funcionalidades estão ativadas.

4.9.3. Considera-se tecnicamente viável a Solução 03 pelas necessidades de equipamentos para atenderem as demandas de segurança e gestão da rede da SEDUC, tendo em vista a descontinuidade dos serviços contratados, haja vista que os contratos de garantia estão com suporte expirados, conforme consta no Processo SEI nº 0029.135533/2020-45, CONTRATO N° 299/PGE-2020 (0012423252). Além de oferecer um nível maior de segurança à rede, os firewall de aplicação, com uma maior capacidade de processamento, possibilitam a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso, seria possível ter uma visualização detalhada da utilização das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças são facilitados e permitem a aplicação de políticas de segurança mais eficientes.

4.9.4. Pelas razões supracitadas essa solução , adequada e a solução viável mostrou-se viável e completa para atendimento às necessidades de segurança cibernética da Secretaria de Educação do Estado de Rondônia.

4.9.5. A solução a ser adquirida enquadra-se na classificação de comum, nos termos do inciso XIII do art. 6º da Lei 14.133/21, levando em consideração a apresentação de especificações técnicas conhecidas e usualmente utilizadas no mercado, não havendo grandes variações qualitativas que demandem análise específica

e diferenciada do particular que pretende contratar com a Administração.

4.9.6. Desta forma, a estrutura procedimental da modalidade pregão - SRP, menos formalista e mais célere, não afeta a análise da qualidade do objeto licitado ou importa em prejuízos ao interesse público.

4.9.7. Por fim, ressaltamos que os serviços pretendidos são de caráter continuado, com todos os insumos para sua autossuficiência, de forma que e o custo total da demanda estará limitado ao valor global da contratação.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

5.1. A descrição da solução como um todo encontra-se pormenorizada no Estudo Técnico Preliminar 47 (70175357) e no Documento de Formalização de Demanda DFD 202 (0056682019).

6. REQUISITOS DA CONTRATAÇÃO (ART. 6º, XXIII, ALÍNEA 'D' DA LEI Nº 14.133/21):

6.1. Sustentabilidade:

6.1.1. 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:

6.1.2. O fiscal avaliará, para efeitos de cumprimento das obrigações contratuais, o que tange a responsabilidade da contratada quanto ao devido recolhimento e o adequado descarte dos itens utilizado na prestação dos serviços, cuja a má destinação poderá causar grande impacto ao meio ambiente (óleos lubrificantes, baterias e pneus).

6.1.3. Priorizar o emprego de mão de obra, materiais, tecnologias e matérias- primas de origem local, nos termos dos incisos II e IV do art. 4º do Decreto nº 7.746/2012;

6.1.4. Obedecer às normas técnicas, de saúde, de higiene e de segurança do trabalho, de acordo com as normas do Ministério do Trabalho e Emprego e normas ambientais vigentes;

6.1.5. Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH nº 4, de11 de maio de 2016;

6.1.6. Não ter sido condenada, a empresa vencedora ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta à previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto n° 5.017, de 12 de março de 2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nºs 29 e 105.

6.2. Subcontratação:

6.2.1. Não será admitida a subcontratação do objeto contratual.

6.2.2. Para o objeto dos autos, não foi facultado subcontratação, cessão e/ou transferência total ou parcial, em razão da necessidade de manter a padronização dos serviços, especialmente por se tratar de serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações We.

6.2.3. A vedação à subcontratação, cessão ou transferência do objeto da contratação está fundamentada em aspectos de segurança da informação, confidencialidade, controle da execução, qualidade dos serviços e conformidade com as exigências legais e normativas, em especial a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018), o Decreto nº 28.874/2024, a IN SGD/ME nº 94/2022 e o art. 72 da Lei nº 14.133/2021.

6.2.4. A segurança da informação é um requisito fundamental nas contratações de TIC, especialmente quando envolvem a manipulação de dados institucionais, integração de equipamentos à rede, acesso a sistemas críticos e tratamento de informações sensíveis. A subcontratação pode expor a instituição a riscos de vazamento de informações, acesso não autorizado, perda de controle sobre os dados e comprometimento da integridade, confidencialidade e disponibilidade das informações, em desacordo com as políticas de segurança da informação e com as exigências da LGPD.

6.2.5. A confidencialidade das informações institucionais deve ser preservada em todas as etapas da contratação, desde a entrega dos equipamentos até a sua integração, operação e manutenção. A subcontratação pode comprometer a confidencialidade, ao permitir o acesso de terceiros não autorizados a informações sensíveis, em desacordo com o art. 6º da IN SGD/ME nº 94/2022 e as diretrizes de segurança da informação estabelecidas no Decreto nº 28.874/2024.

6.2.6. O controle da execução contratual é facilitado quando a empresa contratada é a única responsável pela execução do objeto, permitindo a fiscalização direta, a responsabilização objetiva, a rastreabilidade das ações e a aplicação efetiva de penalidades em caso de descumprimento contratual. A subcontratação pode dificultar a fiscalização, fragmentar a responsabilidade, gerar conflitos de interesse e comprometer a qualidade dos serviços prestados.

6.2.7. A vedação à subcontratação também assegura que a empresa contratada detenha a expertise, os recursos humanos, tecnológicos e financeiros necessários para o cumprimento integral das obrigações contratuais, evitando riscos de execução inadequada, fragmentada ou de baixa qualidade. Essa medida está alinhada ao princípio da eficiência, previsto no art. 5º da Lei nº 14.133/2021, e às melhores práticas de gestão de contratos de TIC.

6.2.8. Portanto, a vedação à subcontratação, cessão ou transferência do objeto é medida necessária para garantir a segurança, a confidencialidade, o controle efetivo da execução contratual, a qualidade dos serviços e a conformidade com as exigências legais e normativas aplicáveis.

6.3. Garantia da Execução (art. 92, XII):

6.3.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133/21, no percentual de 5% do valor contratual, conforme regras previstas no contrato, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual.

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

6.3.3. No caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.

6.3.4. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).

6.3.5. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, na forma da Lei n° 14.133/2021.

6.3.6. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

- prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
- multas moratórias e punitivas aplicadas pela Administração à contratada;

6.3.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

6.3.8. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

6.3.9. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos soba forma escritural, mediante registro em sistema centralizado

de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

6.3.10. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

6.3.11. **A espécie Título de Capitalização, será aceita na modalidade Instrumento de Garantia, como regra geral e deverá ser prestada por ocasião da assinatura do Termo de Contrato, como adimplemento da obrigação contratual a prestação do serviço, na forma prevista no § 7º, art. 92, da Lei nº 14.133/2021.**

6.3.12. O Título de Capitalização, poderá ser aceito inclusive nas hipóteses previstas na alínea "d", II do caput do art. 124 da Lei 14.133/2021.

6.3.13. O Título de Capitalização, será custeado por pagamento único, com resgate pelo valor total e deverão conter o critério de atualização de valores inerentes ao contrato, observadas as normas em vigor.

6.3.14. Para prestação de Garantia por meio de Título de Capitalização, o licitante vencedor deverá em documento específica a cessão total dos direitos do título à contratante, mediante comunicação escrita a sociedade de capitalização ficando vedada a cobrança de qualquer espécie.

6.4. **Do Reajustamento em Sentido Restrito:**

6.4.1. Os preços são fixos e irreajustáveis no prazo de um ano e quando ocorrer reajustamento será com base no Índice de Custos de Tecnologia da Informação - ICTI, **contado da data do orçamento estimado**, conforme § 7º, art. 25, da Lei n. 14.133/2021**.**

6.4.2. As alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei n° 14.133/2021 e arts. 142 a 145 do Decreto Estadual nº 28.874/204.

6.4.3. Os acréscimos ou supressões não poderão exceder a 25% (vinte e cinco por cento) do valor inicial atualizado do contrato nas obras, nos serviços ou nas compras e de 50% (cinquenta por cento), no caso de reforma de edifício ou de equipamento.

6.4.4. O reequilíbrio econômico-financeiro se dará sob a forma de **reajuste em sentido estrito,** espécie de reajuste nos contratos de obra, fornecimento ou serviço continuado sem dedicação exclusiva de mão de obra, com a previsão de índices específicos ou setoriais, ou por **repactuação**, que deverá ser utilizada nas contratações de serviços continuados com regime de dedicação exclusiva de mão de obra, com demonstração analítica da variação dos componentes dos custos, por meio de apresentação da planilha de custos e formação de preços, ou do novo acordo, convenção ou sentença normativa que fundamenta a repactuação.

6.4.5. O pedido relacionado ao reequilíbrio econômico-financeiro deverá ser apresentado pela contratada no prazo máximo de 30 (trinta) dias, contados do fato gerador de seu direito.

6.4.6. Eventual pedido de reajuste ou repactuação seguirá as regras do arts. 150 a 156, do Decreto Estadual nº 28.874/2024.

6.4.7. A **revisão contratual** (revisão de preços ou recomposição) é cabível diante de fatos supervenientes à formulação da proposta e externos à relação contratual, imprevisíveis ou previsíveis, mas de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual, podendo se dar tanto a favor do contratado quanto da Administração contratante, devendo ser instruído com os documentos estabelecidos no art. 164 do Decreto Estadual nº 28.874/2024.

6.4.8. **A decisão sobre o pedido de restabelecimento do equilíbrio econômico-financeiro** (reajuste, repactuação ou revisão) deve ser realizada no **prazo máximo de 60 (sessenta dias)**, contados a partir da solicitação e da entrega dos documentos necessários a instrução do pedido.

6.5. **Da Metodologia de Aplicação:**

6.5.1. A gestão do projeto de contratação de equipamentos de TIC será realizada com base em metodologias reconhecidas de gestão de projetos e análise de riscos, em conformidade com o art. 11 da IN SGD/ME nº 94/2022 e as melhores práticas internacionais, como PMBOK (Project Management Body of Knowledge), PRINCE2 e ISO 31000.

6.5.2. A metodologia PMBOK será utilizada para estruturar o projeto, com definição de escopo, cronograma, marcos, entregas, responsáveis, recursos, custos, riscos e indicadores de desempenho. O uso de uma abordagem estruturada de gestão de projetos permite o acompanhamento sistemático do progresso, a identificação de desvios, a adoção de medidas corretivas tempestivas e a comunicação eficaz entre as partes interessadas. O cronograma do projeto será elaborado com base em técnicas de planejamento, como o método do caminho crítico (CPM), e será monitorado por meio de ferramentas de gestão de projetos, como MS Project ou similares.

6.5.3. A análise de riscos será realizada com base na metodologia da ISO 31000, envolvendo as etapas de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos associados à contratação. Serão considerados riscos de atraso na entrega, não conformidade técnica, indisponibilidade de equipamentos, falhas de integração, riscos ambientais, riscos de segurança da informação e riscos contratuais. Para cada risco identificado, serão definidos planos de resposta, responsáveis, prazos e indicadores de monitoramento, promovendo a mitigação proativa dos impactos negativos e a maximização das oportunidades.

6.5.4. A governança do projeto será assegurada por meio do acompanhamento por comitê gestor de TIC, conforme diretrizes do Decreto nº 28.874/2024, promovendo o alinhamento estratégico, a transparência, a prestação de contas e a participação das partes interessadas. O comitê gestor será responsável por aprovar o plano de projeto, monitorar o progresso, deliberar sobre questões críticas, aprovar mudanças de escopo e garantir a aderência às políticas institucionais de TIC.

6.5.5. A adoção dessas metodologias contribui para o sucesso da contratação, mitigando riscos, promovendo o controle efetivo, assegurando a entrega dos resultados esperados e alinhando o projeto às melhores práticas de governança, gestão de riscos e compliance.

6.5.6. Além das metodologias já mencionadas, destaca-se que a aplicação de boas práticas de gestão de projetos em contratações de TIC é uma exigência crescente dos órgãos de controle e um diferencial para o sucesso das iniciativas públicas. O uso do PMBOK, por exemplo, permite a formalização de processos de iniciação, planejamento, execução, monitoramento, controle e encerramento do projeto, garantindo que todas as etapas sejam devidamente documentadas e auditáveis. O detalhamento do escopo, aliado à Estrutura Analítica do Projeto (EAP), facilita a decomposição das entregas em pacotes de trabalho gerenciáveis, promovendo maior clareza na atribuição de responsabilidades e no acompanhamento do progresso.

6.5.7. A integração de metodologias ágeis, como Scrum ou Kanban, pode ser considerada em etapas específicas do projeto, especialmente naquelas que envolvem customização, desenvolvimento de soluções ou ajustes finos pós-implantação. Essa abordagem híbrida, reconhecida pelo PMI e por órgãos como o TCU, permite maior flexibilidade, adaptação a mudanças e entregas incrementais de valor, sem perder o controle e a rastreabilidade proporcionados pelas metodologias tradicionais.

6.5.8. No que tange à análise de riscos, a ISO 31000 orienta não apenas a identificação e o tratamento de riscos, mas também a criação de uma cultura organizacional voltada à prevenção e à resiliência. O registro dos riscos em matriz específica, com avaliação de probabilidade, impacto e estratégias de resposta, será atualizado periodicamente e compartilhado com as partes interessadas, promovendo a transparência e a tomada de decisão baseada em evidências. Riscos relacionados à sustentabilidade, à conformidade ambiental, à proteção de dados pessoais (LGPD) e à continuidade dos serviços também serão monitorados, em consonância com as diretrizes do ETP e do Plano Diretor de TIC.

6.5.9. A governança do projeto será fortalecida pela adoção de mecanismos de prestação de contas, reuniões de acompanhamento (status report), checkpoints de validação de entregas e registro de lições aprendidas. O comitê gestor de TIC, além de monitorar o progresso, será responsável por deliberar sobre eventuais mudanças de escopo, aprovar replanejamentos e garantir que as decisões estejam alinhadas ao planejamento estratégico institucional e às políticas de governança, conforme previsto no Decreto nº 28.874/2024 e nas recomendações do TCU (Acórdão nº 2.622/2015-Plenário).

6.5.10. A comunicação será tratada como um fator crítico de sucesso, com a elaboração de um plano de comunicação que defina fluxos, periodicidade, canais e públicos-alvo das informações do projeto. Serão promovidas reuniões regulares com stakeholders, divulgação de marcos alcançados e relatórios executivos para a alta administração, assegurando o engajamento e a transparência em todas as fases.

6.5.11. Outro aspecto relevante é a preocupação com a sustentabilidade e a inovação. O projeto buscará incorporar práticas de Green IT, priorizando soluções energeticamente eficientes, com menor impacto ambiental e maior potencial de reutilização e reciclagem, em consonância com a legislação vigente e as políticas institucionais de responsabilidade socioambiental.

6.5.12. Por fim, a adoção dessas metodologias e práticas de governança, gestão de riscos, compliance, comunicação e sustentabilidade não apenas atendem às exigências normativas, mas também contribui para a maturidade institucional, a eficiência na aplicação dos recursos públicos e a geração de valor para a sociedade. O registro e a disseminação das lições aprendidas ao final do projeto servirão de base para o aprimoramento contínuo dos processos de contratação e gestão de projetos de TIC na instituição.

7. GLOSSÁRIO DE TERMOS ESPECÍFICOS DE TIC:

- **WAF (Web Application Firewall):** Firewall de Aplicações Web. Solução de segurança projetada para proteger aplicações web contra ataques como XSS, SQL Injection, CSRF e outros listados no OWASP Top 10.
- **Appliance**: Equipamento físico dedicado a executar funções específicas de segurança de rede, como firewall, WAF ou balanceamento de carga.
- **Alta disponibilidade (HA):** Configuração de sistemas redundantes para garantir continuidade do serviço em caso de falhas em um ou mais componentes do sistema.
- **Camada 7:** Referente à camada de aplicação do modelo OSI, onde operam protocolos como HTTP, DNS, SMTP e FTP. É onde ocorrem ataques como XSS e SQLi.
- **Camada 4**: Refere-se à camada de transporte do modelo OSI, onde operam os protocolos TCP e UDP.
- **TLS (Transport Layer Security):** Protocolo de segurança que criptografa a comunicação entre servidores e clientes, garantindo confidencialidade e integridade dos dados.
- **SSL Offload:** Técnica que transfere a carga de criptografia SSL/TLS do servidor de aplicação para o appliance, melhorando a performance do servidor.
- **DDoS (Distributed Denial of Service):** Ataques distribuídos que visam sobrecarregar sistemas, tornando os serviços indisponíveis. O WAF ajuda na mitigação desses ataques.
- **SYN Flood:** Tipo de ataque DoS que explora o processo de handshake TCP para consumir recursos do servidor.
- **Tenants**: Instâncias ou ambientes independentes dentro de uma mesma infraestrutura de solução, com dados e configurações isolados.
- **SNMP (Simple Network Management Protocol):** Protocolo para monitoramento e gerenciamento de dispositivos de rede. Inclui versões v1, v2c e v3.
- **NetFlow / sFlow / IPFIX:** Protocolos de exportação de dados de fluxo de tráfego de rede usados para análise e monitoramento de performance e segurança.
- **Prometheus:** Sistema de monitoramento e alerta de métricas de desempenho, usado amplamente em ambientes de TI modernos.
- **Cluster:** Conjunto de equipamentos ou servidores que operam em conjunto, como se fossem um único sistema, para garantir desempenho e redundância.
- **VXLAN (Virtual Extensible LAN)**: Tecnologia de encapsulamento que permite criar redes virtuais sobre redes físicas para uso em ambientes de virtualização.
- **RADIUS, LDAP, TACACS+, Active Directory:** Protocolos e serviços utilizados para autenticação centralizada de usuários em redes corporativas.
- **Syslog**: Protocolo para envio de logs de eventos e mensagens do sistema para servidores centralizados.
- **OWASP Top 10:** Lista das dez principais vulnerabilidades de segurança em aplicações web, publicada pela OWASP (Open Web Application Security Project).
- **NAT (Network Address Translation):** Técnica que permite reescrever os endereços IP de pacotes que trafegam por um roteador ou firewall.
- **SNI (Server Name Indication)**: Extensão do protocolo TLS que permite múltiplos certificados SSL em um único endereço IP.
- **JSON / XML**: Formatos de dados usados amplamente para comunicação entre sistemas via APIs. A proteção contra ataques nesses formatos é essencial.
- **OpenAPI**: Especificação padrão para descrever APIs RESTful, usada para facilitar a integração entre sistemas e segurança de endpoints.
- **SPA (Single Page Application):** Aplicações web que carregam uma única página HTML e atualizam dinamicamente o conteúdo sem recarregar a página inteira.
- **Captcha / JavaScript Challenge:** Mecanismos usados para diferenciar usuários humanos de bots durante acessos web.
- **Credential Stuffing**: Técnica de ataque que tenta acessar sistemas reutilizando credenciais (usuário/senha) obtidas em vazamentos anteriores.
- **GeoIP / Geolocalização IP:** Técnica de mapeamento de endereços IP para localização geográfica, usada para criar políticas de acesso baseadas em país ou região.
- **DoH (DNS over HTTPS)**: Protocolo que encapsula consultas DNS sobre HTTPS, proporcionando mais privacidade e segurança.
- **Ingress / LoadBalancer / Route:** Objetos usados em plataformas de orquestração (como Kubernetes/OpenShift) para publicar serviços para o mundo externo.
- **ICAP (Internet Content Adaptation Protocol):** Protocolo que permite inspeção de conteúdo (ex: antivírus, DLP) em tempo real nos uploads de arquivos.
- **SCTP (Stream Control Transmission Protocol):** Protocolo de transporte usado principalmente em aplicações de telefonia IP e sinais de telecomunicações.
- **MITM (Man-In-The-Middle)**: Ataques onde o invasor intercepta e possivelmente altera a comunicação entre duas partes sem que elas saibam.
- **IPSec**: Conjunto de protocolos para proteger comunicações IP por meio de autenticação e criptografia de pacotes IP.
- **Red Team / Blue Team** : Equipes envolvidas em testes de segurança ofensiva (Red Team) e defensiva (Blue Team) para validar e melhorar a segurança de sistemas.

7.1. Detalhamento do objeto:

7.1.1. Características de desempenho e escalabilidade da unidade básica da solução:

1. Possuir capacidade mínima para tratar 60 (sessenta) Gbps de throughput em Camada 7;
2. Possuir capacidade mínima para tratar 95 (noventa e cinco) Gbps de throughput em Camada 4;
3. Possuir capacidade de compressão em Hardware de 35 (trinta e cinco) Gbps;
4. Possuir capacidade de manter, no mínimo, 75.000.000 (setenta e cinco milhões) de conexões simultâneas na camada 4;
5. Ter capacidade de receber 1.000.000(um milhão) novas conexões em camada 4 por segundo;
6. Possuir capacidade de Proteção DDoS em Hardware de 80.000.000 (oitenta milhões) SYN cookies por segundo;
7. Processar 30.000 (trinta mil) transações por segundo TLS com RSA 2K;
8. Possuir capacidade e estar licenciado para até 08 tenants;
9. A solução deverá ser entregue em Appliance Físico e não será aceito a composição em equipamentos menores para alcançar os requisitos solicitados;
10. A solução deverá ser fornecida com no mínimo 08 (oito) interfaces 25G com os respectivos transceivers;
11. Os equipamentos desta solução devem ser equipamentos físicos de mesmo fabricante, modelo, versão e licenciamento, sendo essa exigência requisito técnico fundamental para configuração de dispositivos que operarão em modo cluster;

12. O hardware e software que executarão os recursos e funcionalidades dessa camada de proteção deverão ser do tipo appliance físico, com hardware e software desenvolvidos para essa finalidade;
13. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
14. A solução deve ser entregue com licenciamento perpétuo, com garantia e suporte técnico por 60 meses;
15. A solução deve permanecer plenamente operante após o fim da garantia contratada, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência;
16. A solução deve ser entregue com fonte redundante;

7.1.2. **Requisitos gerais:**

1. Suportar IPv4 e IPv6;
2. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;
3. Suportar VXLAN para integração com o ambiente de virtualização;
4. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;
5. Suportar implementação em alta disponibilidade,
6. Implementar modo ativo/standby;
7. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;
8. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;
9. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, hearbeat e sincronização entre os equipamentos;
10. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;
11. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;
12. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;
13. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
14. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;
15. Manter internamente múltiplos arquivos de configurações do sistema;
16. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;
17. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;
18. Permitir a configuração de múltiplas contas locais de administradores;
19. Implementar controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;
20. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;
21. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;
22. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;
23. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;
24. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
25. Suportar a rollback de configuração e imagem;
26. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;
27. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;
28. Permitir reiniciar o equipamento pela interface gráfica e por CLI;
29. Implementar SNMPv1, SNMPv2c e SNMPV3;
30. Implementar traps SNMP;
31. Permitir a criação de MIBs customizadas;
32. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events
33. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:
34. Coleta de métricas de desempenho compatível com Prometheus;
35. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;
36. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, ElasticSearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka, Splunk e StatsD;
37. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;
38. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;
39. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;
40. Deve incluir métricas de throughtput, conexões, bits, pacotes, disponibilidade;
41. Deve incluir métricas de requisições, respostas;
42. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;
43. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;
44. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;
45. Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;
46. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);
47. Deve incluir métricas do cluster, incluindo data de sincronização;
48. Deve incluir informações de data da última configuração aplicada;

49. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;
50. Implementar debugging utilizando CLI via console e SSH;
51. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;
52. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou MacOS;
53. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size
54. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;
55. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;
56. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;
57. Implementar roteamento IPv4 e IPv6 estático e dinâmico;
58. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;
59. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
60. Suportar integração via BGP para divulgação de prefixos;
61. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;
62. Suportar Equal Cost Multipath (ECMP);
63. Implementar Bidirectional Forward Detection (BFD);
64. Implementar funções de entrega de aplicações através do balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;
65. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;
66. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;
67. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;
68. Implementar criptografia de cookies;
69. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;
70. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de servidores;
71. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;
72. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;
73. Suportar balanceamento de carga de servidores SIP para VoIP;
74. Permitir limitar o número de conexões estabelecidas com cada servidor real;
75. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;
76. Implementar Network Address Translation (NAT) do IP do servidor;
77. Implementar Network Address Translation (NAT) do IP do cliente;
78. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;
79. Implementar proteção contra SYN floods;
80. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;
81. Suportar multiplexação TCP e reuso de sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;
82. Suportar Stream Control Transmission Protocol (SCTP);
83. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;
84. Permitir recriptografar a conexão entre a solução e o servidor;
85. Permitir espelhamento de tráfego de conexões TLS;
86. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;

7.1.3. **Em relação ao tráfego TLS, deve suportar:**

1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;
2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;
3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;
4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;
5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;
6. Suportar os algoritmos para sessões TLS:
7. SSL session cache Timeout;

8. Session Ticket;
9. OCSP (Online Certificate Status Protocol) Stapling;
10. Dynamic Record Sizing;
11. ALPN (Application Layer Protocol Negotiation);
12. Perfect Forward Secrecy;
13. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);
14. Suportar importação de certificados digitais e chaves privadas;
15. Possuir alertas visuais na interface web de certificados com vencimento próximo;
16. Implementar limpeza de cabeçalho HTTP;
17. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;
18. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;
19. Permitir as ações para o tráfego classificado: bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;
20. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;
21. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;
22. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;
23. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;
24. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração;
25. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;
26. Permitir a configuração através de ConfigMaps;
27. Permitir a configuração através de CustomResourceDefinition (CRD) da solução;
28. Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;
29. Permitir a configuração através de objetos Ingress na plataforma;
30. Permitir a configuração através de objetos Route no OpenShift;
31. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;
32. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada;
33. Suportar o protocolo FTP com, pelo menos, as seguintes características:
34. Determinar os comandos FTP permitidos;
35. Requests FTP anônimos;
36. Validar conformidade com o protocolo FTP;
37. Proteger contra ataques de força bruta nos logins;
38. Suportar o protocolo SMTP com, pelo menos, as seguintes características
39. Limitar o número de mensagens;
40. Validar registro SPF do DNS;
41. Determinar quais métodos SMTP podem ser utilizados.
42. Implementar proteção de aplicações no nível de rede e protocolo;
43. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio;
44. Proteger de ataques DDoS nas camadas de rede e de sessão;
45. Proteger de ataques DDoS que utilizem SSL;

7.1.4. **A solução deve permitir a criação de regras com, no mínimo, os parâmetros:**

1. Endereço IP de destino
2. Endereço IP de origem
3. Porta de destino
4. Porta de origem
5. VLAN
6. Protocolo
7. Ação
8. Horário
9. Log;
10. Permitir definir agendamento para ativação da regra;
11. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;
12. Implementar a descoberta automática de serviços presentes em objetos monitorados;
13. Permitir definir, no mínimo, as seguintes ações no tráfego:
14. Permitir: os pacotes são aceitos e passam pela solução;
15. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;

16. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;
17. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:
18. Global, regras válidas para todo o tráfego, independente da interface de ingresso;
19. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;
20. Objeto, regras válidas para objetos específicos;
21. Deve possuir criptografia IPSEC para comunicação entre sites;
22. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;
23. Permitir a restauração das configurações de proteções originais;
24. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-rede;
25. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;
26. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;
27. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;
28. Permitir a criação de regras de filtragem através de API REST declarativa;
29. A documentação da API deve ser pública;
30. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito
31. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;
32. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, BadIGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;
33. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;
34. Limitar o número de consultas DNS por segundo através da configuração de limiares;
35. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;
36. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;
37. Suportar envio de SNMP traps para cada ataque DoS detectado;
38. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;
39. Deve possuir a funcionalidade de limiares automático para vetores de DoS:
40. Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.
41. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;
42. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;
43. Suportar integração com serviço de tratamento de DDoS externo através do compartilhamento de informação de vetores e sinalização de ataques em andamento para redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos;

7.1.5. **Implementar serviços de entrega de aplicações distribuídas através do serviço de DNS:**

1. Implementar serviços de DNS com as funções de DNS autoritativo, DNS secundário, DNS resolver, DNS cache e balanceamento de servidores de DNS;
2. Implementar DNSSec, independente da estrutura dos servidores DNS em uso;
3. Implementar transferência de zonas para múltiplos servidores DNS primários responsáveis por diferentes zonas;
4. Suportar uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;
5. Implementar offload dos servidores de DNS, funcionando como o DNS secundário;
6. Implementar proteções contra-ataques DNS, incluindo no mínimo a inspeção de protocolo, validação de protocolo, UDP flood, pacotes malformados, teardrop e DNS Water-torture;
7. Permitir a criação de códigos ou scripts que possam manipular as respostas de DNS;
8. Implementar filtragem de pacotes e tipos de requisições;
9. Implementar segurança do protocolo DNS, protegendo de ataques de negação de serviço, NXDOMAIN, reflexão e amplificação de DNS e Cache Poisoning;
10. Implementar stateful inspection das requisições e respostas de DNS;
11. Possuir base de geolocalização IP;

7.2. **Implementar DNS64 e implementar as seguintes integrações:**

1. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A e AAAA e responde com um prefixo + A e AAAA
2. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A, caso não tenha resposta, faz a consulta com AAAA, responde para o cliente um prefixo + A e AAAA
3. Cliente envia consulta AAAA, a solução encaminha uma consulta (recursivo) como A e responde um prefixo + AAAA
4. Implementar filtros para tipos de requisição, de forma que apenas as operações e requisições autorizadas sejam encaminhadas para os servidores de DNS.
5. Suportar pelo menos os tipos de requisição SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT, DS, CAA e DNSKEY;
6. Suportar DNS over HTTPS (DoH);
7. Permitir a criação de resoluções de DNS com tratamento diferenciado de consultas conforme origem das requisições;

8. Apresentar estatísticas sobre consultas de DNS por aplicação, nome da query, tipo da query, endereço IP do cliente;
9. Implementar modo inline na estrutura de DNS existente e transparente;
10. Suportar IP Anycast;
11. Implementar alta disponibilidade sem depender de BGP ou outro protocolo de roteamento;
12. Implementar alta disponibilidade de Data Centers e serviços baseada em respostas a requisições DNS, de forma que a resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;
13. Suportar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;
14. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;
15. Suportar monitores utilizando HTTPS, incluindo a validação do SNI;
16. Suportar pelo menos os algoritmos de balanceamento Round Robin, Global Availability, Ratio, LDNS Persist, Geografia, round trip time e hops;
17. Implementar persistência da conexão do usuário entre aplicações ou data centers;
18. Suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;
19. Permitir que as políticas sejam configuradas individualmente por aplicação que será balanceada;
20. Permitir que a contingência seja automática;
21. Permitir o retorno do Data Center de forma automática e manual;
22. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requisições AAAA);
23. Possuir suporte a IPv6 no balanceamento global entre datacenters;
24. Possuir a funcionalidade de resposta rápida a requisições de DNS, permitindo respostas mais rápidas para zonas que seja autoritativo;
25. Suportar Response Policy Zones (RPZ), mecanismo de proteção de resolução para DNS recursivo que permite o tratamento customizado da resolução de nomes, capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas;
26. Suportar EDNS-Client-Subnet (ECS) para tanto responder requisições de clientes para balanceamento de Data Center ou encaminhar requisições de clientes.
27. Implementar a utilização da subnet do cliente presente no ECS para tomada de decisão de balanceamento de Data Center, independente do endereço do LDNS;
28. Suportar inserir o ECS para outros servidores DNS;
29. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver, deve ser usada a persistência existente para manter o cliente no mesmo Data Center;
30. Permitir consultar a resposta de uma resolução de DNS em uma base de IP e permitir que a resposta seja alterada antes de ser enviada para o cliente;
31. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso, incluindo IP de origem, destino, data e hora do acesso.
32. Suportar, no mínimo, as ações de apenas registrar, bloquear o dado ou substituir o nome do domínio;
33. Permitir configurar rate limit realizadas via TCP ou UDP por FQND;
34. Permitir configurar rate limit para consultas realizadas via TCP ou UDP por IP de origem;
35. Implementar proteção para aplicações web e API contra ameaças na camada de aplicação;
36. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;
37. Implementar ajustes automáticos e adaptativos de limiares de DoS;
38. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;
39. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;
40. Implementar modelo positivo de segurança de aplicações web;
41. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;
42. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;
43. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
44. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
45. Permitir desativar a inspeção para URL específicas;
46. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;
47. Permitir a integração com firewall de banco de dados;
48. Suportar aplicações que utilizam protocolo WebSocket;
49. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, para comunicação com o cliente e comunicação com o servidor, sem a necessidade de downgrade de versão;
50. Implementar proteção contra:
51. Acesso por força bruta;
52. DoS e DDoS em camada 7;
53. Buffer Overflow;
54. Cross Site Request Forgery (CSRF);
55. Cross-Site Scripting (XSS);
56. Server-Side Request Forgery (SSRF);
57. SQL Injection;
58. Parameter tampering;
59. Cookie poisoning;

60. HTTP Request Smuggling;
61. Manipulação de campos escondidos (hidden input);
62. Manipulação de cookies;
63. Roubo de sessão através de manipulação de cookies;
64. Sequestro de sessão;
65. Validação de consistência de formulários;
66. Validação do cabeçalho do “user-agent” para identificar clientes inválidos;
67. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);
68. Suportar codificação HTML "application/x-www-form-urlencoded";
69. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;
70. Suportar codificação fragmentada (chunked encoding);
71. Suportar validações de protocolo:
72. Restrição de métodos;
73. Restrição de protocolos e versões;
74. Validação de conformidade com RFCs;
75. Validação de caracteres URL-encoded;
76. Validação de codificação fora de padrão %uXXYY.
77. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;
78. Possuir técnicas de detecção de evasões:
79. URL-decoding;
80. Terminação Null Byte String;
81. Paths autorreferenciados;
82. Case de caracteres misturados;
83. Uso excessivo de espaços em branco;
84. Decodificação de entidades HTML;
85. Caracteres de escape;
86. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);
87. Capacidade de filtrar cabeçalhos, corpo e status de respostas;
88. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
89. Implementar validação de URL;
90. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;
91. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;
92. Suportar aplicações Single-Page Application (SPA);
93. Permitir a customização da resposta de bloqueio;
94. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;
95. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;
96. Implementar as proteções:
97. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;
98. Ocultar qualquer mensagem de erro HTTP dos usuários;
99. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
100. Suportar políticas por geolocalização para restrição de acesso a determinados países;
101. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;
102. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;
103. Implementar aprendizado automático de XML;
104. Permitir a importação de arquivo de esquema XML;
105. Implementar aprendizado automático de JSON;
106. Permitir a importação de arquivo de esquema JSON;
107. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;
108. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
109. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;
110. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;
111. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;
112. A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas;
113. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;
114. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;
115. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas

informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;

116. Possuir assinaturas de ataques para conteúdo em JSON e XML;
117. Possuir proteções contra XML Bomb;
118. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;
119. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;
120. Implementar detecção de DoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;
121. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;
122. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;
123. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;
124. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;
125. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);
126. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;
127. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;
128. Implementar mitigações para ataques DoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;
129. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;
130. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação;
131. Identificar ataques com diferentes usuários e mesma origem;
132. Identificar ataques com diferentes origens e mesmo usuário;
133. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;
134. Possuir funcionalidade para integração com listas externas de credenciais expostas para mitigar ataques Credential Stuffing e Password Sprawl;
135. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;
136. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;
137. Implementar detecção e mitigação para proteção contra bots através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise;
138. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;
139. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.
140. Possuir atualização automática de definição de bots;
141. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;
142. Permitir a criação de definições de bots;
143. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;
144. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;
145. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;
146. Permitir configurar exceções as regras de rate limits para chamadas na API;
147. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);
148. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;
149. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;
150. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;
151. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;
152. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;
153. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;
154. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;
155. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;
156. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;
157. Implementar um identificador único para cada requisição tratada pela solução;
158. Permitir o armazenamento local de eventos e exportação para servidores externos;
159. Permitir configurar a retenção dos eventos por tempo e volume;
160. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;
161. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);
162. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;
163. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;

164. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;
165. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;
166. Suportar integração com funcionalidade de gestão avançada de tráfego automatizado para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador;
167. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;
168. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

7.2.1. **Implementar bases de inteligência de ameaças atualizadas automaticamente:**

1. A solução deve implementar a atualização das bases de inteligência de ameaças para proteção de DoS/DDoS, serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API durante a vigência do contrato;
2. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiro homologado através de assinaturas de serviços próprios;
3. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;
4. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;
5. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS e serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API;
6. Permitir utilizar a base de inteligência de IP durante consultas de DNS, permitir ações diferentes configuradas de acordo com a categoria e alterar a resposta antes de ser enviada para o cliente na solução de proteção de DDoS e serviços de DNS;
7. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;
8. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho X-Forwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;
9. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real;
10. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;
11. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;
12. Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;
13. Devem ser automáticas e frequentes as atualizações de regras, políticas, configurações e demais ajustes que dependem do serviço de inteligência, sem interrupção do serviço, sem necessidade de atualização do sistema operacional e nem reiniciar o equipamento a cada atualização

7.2.2. **Identificação e Acesso:**

1. Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com no mínimo os seguintes recursos:
2. Deve possuir o modo “Portal” onde a solução se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;
3. Deve possuir o modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna.
4. Deverá possuir ativo o controle de, no mínimo, 500 usuários concorrentes, e deverá vir com todo o licenciamento necessário para ativação desses 500 usuários;
5. Deverá possuir cliente VPN SSL para pelo menos os sistemas operacionais Windows, Linux e MacOS;
6. Deverá possuir validação da estação de trabalho do usuário, para pelo menos: Sistema Operacional, Antivírus e Firewall.
7. Deverá ser capaz de autenticar usuários em, pelo menos, bases de dados:
8. LDAP
9. Radius
10. TACACS+
11. Active Directory;
12. Deve possuir capacidade para realizar múltiplos métodos de autenticação remotos, incluindo pelo menos:
13. Radius
14. LDAP
15. Active Directory
16. TACACS+
17. Kerberos;
18. Deve possuir capacidade para permitir a troca da senha dos usuários que tenham expirado;
19. Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso a rede;
20. Deve possuir capacidade de redirecionar tráfego HTTP para HTTPs para um determinado servidor virtual;
21. Deve possuir capacidade para definir ACLs estáticas e dinâmicas;
22. Deve possuir capacidade para realizar Single Sign On (SSO) utilizando:
23. NTLM
24. Basic
25. HTTP Forms
26. Kerberos

27. OAM;
28. Deve possuir capacidade de utilizar JSON Web Token (JWT) para autorizar e autenticar acesso as aplicações e APIs
29. Deve possuir a capacidade de utilizar JWE, onde o JWT será criptografado e decritptografado utilizando, pelo menos, chaves RSA.
30. Deve possuir capacidade para, graficamente, criar e manter as políticas de acesso como diagrama de fluxo;

7.2.3. **Implementar painéis para monitoramento da solução:**

1. Possuir relatórios do serviço de DNS incluindo tendência de latência de resposta de DNS, nomes de domínios de DNS mais requisitados, tendência de uso do cache de DNS, clientes de DNS, clientes por domínio de DNS, taxa de consultas de DNS por tipo de registro, taxa de consultas de DNS diária por servidor, pico de consultas diárias de DNS por servidor, NXDOMAIN, SERVFAIL enviados e recebidos, nomes de domínios com conteúdo malicioso, principais domínios maliciosos;
2. Possuir relatórios de proteção do serviço de DNS, incluindo eventos por período, eventos por severidade, eventos por regra, eventos por tendência e eventos por categoria;
3. Suportar a exportação de eventos de DNS utilizando IPFIX;
4. Deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS;
5. Possuir relatório de ataques DDoS com indicação de início e fim do ataque;
6. Possuir relatório em tempo real sobre ataques DDoS, atualizado automaticamente;
7. Possuir relatório de ataques DDoS incluindo quantidade de eventos e severidade, ataques por protocolo, incluindo assinaturas utilizadas e serviços mais afetados;
8. Possuir relatórios de ataques DDoS incluindo a origem dos ataques, país, requisições por segundo, gatilho da proteção e mitigação adotada;
9. Suportar a exportação de eventos de DoS utilizando IPFIX;
10. Possuir painel de acompanhamento de adoção de proteções contra ameaças mais comuns, de acordo com OWASP Top 10 2021;
11. Possuir relatório de desempenho da solução, incluindo processamento total e por servidor virtual protegido;
12. Possuir relatórios consolidados de ataques incluindo, pelo menos, resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, ataques DoS, ataques de força bruta, ataques de bots, violações, URL, endereços IP, países e severidade;
13. Possuir relatório de incidentes com violações detectadas e correlacionadas, separando falsos positivos de atividades maliciosas e para facilitar a resposta a incidentes;
14. Implementar monitoração e análise de performance de aplicações web;
15. Possuir relatórios de métricas de aplicações, incluindo transações por segundo, tempo de reposta, latência do cliente e servidor, throughput de requisição e resposta e sessões;
16. Possuir relatórios de análises históricas detalhamento do tempo de resposta total de carregamento de uma URL e página e correlação de métricas de uso de rede com o comportamento das aplicações para auxiliar processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;
17. Possuir relatórios para análise de dados por aplicações, por URL, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;
18. Possuir relatórios para análise de estatísticas de acesso, incluindo métodos HTTP, sistema operacional e navegadores;
19. Permitir exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário
20. Possuir relatório de ataques DoS em camada 7 com indicação de início e fim do ataque;
21. Possuir relatório em tempo real sobre ataques DoS em camada 7, atualizado automaticamente;
22. Possuir relatório que permite avaliar o impacto de ataques DoS em camada 7 na performance do servidor.

7.2.4. **Solução de Segurança Avançada**

1. Cada unidade deste item deve fornecer proteção para no mínimo 20 FQDN’s
2. Cada unidade deste item equivale a 60 meses de subscrição
3. Implementar serviço avançado de proteção de ataques às aplicações web, disponíveis em qualquer infraestrutura pública ou privada, exposta para a Internet, sem limite de usuários, conexões, sessões e transações;
4. Implementar gestão automática de certificados digitais, incluindo a renovação dos certificados, devendo possuir integração com no mínimo o serviço Let's Encrypt (https://letsencrypt.org/);
5. Permitir a gestão manual de certificados através da importação de certificado digital e chave privada da CONTRATANTE, devendo esta ser armazenada em repositório seguro e protegido;
6. Suportar OCSP;
7. Permitir a configuração de múltiplos domínios (FQDN) para a mesma aplicação;
8. Suportar a gestão automática dos certificados de todos os domínios;
9. Suportar a gestão manual de certificados digitais e chaves privadas de todos os domínios;
10. Permitir a configuração de diferentes conjuntos (pools) de servidores de origem da aplicação com algoritmos de balanceamento para escolha do pool;
11. Permitir configurar pesos e prioridades diferentes para cada Pool de Servidores que originam o Tráfego;
12. Permitir configurar um algoritmo de balanceamento de Servidores que originam o Tráfego de um pool diferente do algoritmo de balanceamento de pools;
13. Permitir configurar monitores de disponibilidade de Servidores que originam o Tráfego;
14. Permitir a configuração de diferentes pools de Servidores que originam o Tráfego selecionados a partir de atributos da aplicação, incluindo no mínimo método HTTP, prefixos, expressões regulares da URL e cabeçalhos HTTP;
15. Permitir definir políticas de WAF diferentes por pool;
16. Permitir inserir cabeçalho HSTS (HTTP Strict-Transport-Security);
17. Implementar TLS 1.2 e superiores, com algoritmos fortes e cifras que suportem PFS (Perfect Forward Secrecy);
18. Implementar Mutual TLS (mTLS) com a opção de enviar o certificado do cliente como cabeçalho HTTP para o Servidor de Origem;
19. Permitir especificar a lista de Autoridades Certificadoras (CA) de validação do certificado;

20. Permitir verificar o certificado do cliente em listas de revogação (CRL);
21. Permitir enviar o certificado completo;
22. Permitir enviar atributos específicos do certificado;
23. Suportar HTTP/1.1 e HTTP/2;
24. Implementar inspeção e varredura com base em assinaturas para detecção de requisições maliciosas, incluindo, no mínimo, proteções de:
25. Cross-Site Scripting (XSS);
26. Cross-Site Request Forgery (CSRF);
27. Directory Traversal;
28. Directory Climbing;
29. SQL injection;
30. Cookie Injection;
31. Command Injection;
32. Code Injection;
33. Web Parameter Tampering;
34. Cookie Tampering;
35. Implementar a configuração para identificação e mascaramento de dados sensíveis enviados pelo servidor para o cliente;
36. Implementar detecção e mitigação de violações do protocolo HTTP;
37. Implementar proteção contra exploração de vulnerabilidade (exploit);
38. Implementar proteção contra adulteração de cookies do serviço de proteção de aplicações;
39. Implementar inspeção, descoberta e proteção de requisições que utilizem GraphQL;
40. Permitir a configuração de políticas de segurança de permissão e bloqueio;
41. Permitir a criação de regras de exclusão de forma granular, considerando cookies, parâmetros, cabeçalhos e outros;
42. Permitir a configuração de regras de segurança positiva, onde será definido o que é permitido e todo o restante é rejeitado;
43. Permitir a configuração de políticas e regras que protejam as aplicações de ameaças e vulnerabilidades listadas no OWASP Top 10 e atualizações dessa lista;
44. Implementar proteções de campanhas de ataques e ameaças, informando a ação, o ator e a vulnerabilidade explorada;
45. Permitir criar diferentes políticas de segurança para inspeção e proteção por aplicação;
46. Permitir habilitar uma política de segurança sem bloqueios, ou seja, apenas para geração de alertas ou monitoramento;
47. Implementar mecanismos de ajuste automático de assinaturas ou machine learning para redução de falso-positivos;
48. Implementar fase de preparação de assinaturas de ataque, quando assinaturas novas e atualizadas são configuradas no modo de monitoramento por um período;
49. Permitir desabilitar inspeções para tipos de ataques específicos;
50. Permitir definir os códigos de respostas HTTP (status code) que serão aceitos vindos da aplicação original, quando os demais códigos serão bloqueados;
51. Permitir ocultar atributos e parâmetros sensíveis, tais como senhas ou outros dados sensíveis, em mensagens de log da plataforma;
52. Permitir a criação de diferentes páginas de respostas de bloqueio, fornecendo um identificador de requisição;
53. Permitir a criação de diferentes páginas de respostas por códigos de respostas HTTP (status code);
54. Implementar a identificação de usuários e clientes a partir de informações extraídas de cabeçalhos IP, HTTP, parâmetros, cookies, JWT e fingerprint do TLS;
55. Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem;
56. Implementar limitação de tráfego (rate limit) por usuário;
57. Permitir a criação de regras de bloqueio com base na classificação do IP de origem e sua reputação;
58. Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas de ataques web;
59. Permitir a definição de taxa máxima de requisições (rate limit);
60. Permitir definir uma lista de clientes confiáveis que não serão bloqueados por regras da política de segurança;
61. Permitir definir uma lista de clientes suspeitos que devem ser bloqueados;
62. Implementar a inspeção com base no IP do cliente que iniciou a conexão e permitir utilizar o IP do cliente, o cabeçalho X-Forwarded-For por exemplo, presente no cabeçalho HTTP;
63. Permitir inserir cabeçalho HTTP na requisição e na resposta;
64. Permitir remover cabeçalhos HTTP da requisição;
65. Implementar o redirecionamento automático de HTTP para HTTPS;
66. Permitir a configuração de políticas de CORS (Cross-Origin Resource Sharing);
67. Implementar mitigação automática de DDoS em camada 7;
68. Implementar mitigação automática de ataques "Slow and low";
69. Avaliação de Vulnerabilidades:
70. Implementar serviço de varredura automáticas de vulnerabilidades de aplicações web;
71. Implementar testes de penetração de aplicações totalmente automáticos, ou seja, sem a necessidade de escrita de scripts, roteiros ou playbooks;
72. Implementar identificação, navegação, varredura e testes completos, independentemente da tecnologia da aplicação;
73. Implementar relatórios com a vulnerabilidades encontradas, incluindo capturas de tela, vídeos e detalhes técnicos, permitindo uma compreensão completa;
74. Fornecer relatórios online e em PDF;
75. Informar com detalhes as requisições realizadas que apontaram vulnerabilidades e a resposta da aplicação;

76. Permitir o download da resposta da aplicação;
77. Permitir configuração de alertas a respeito das varreduras e problemas encontrados;
78. Implementar avaliação de exposição de acordo com OWASP Top 10;
79. Fornecer orientações de mitigação e correção dos problemas encontrados;
80. Permitir inserir notas e observações sobre os problemas encontrados;
81. Implementar serviço de varredura de domínios para identificação e análise de aplicações expostas para a Internet;
82. Deve identificar domínios e subdomínios;
83. Deve identificar portas e serviços hospedadas pelos domínios e subdomínios;
84. Deve identificar a aplicação hospedada pelos domínios e subdomínios;
85. Permitir a configuração de varreduras de aplicações de forma automática a partir da descoberta;
86. Permitir a configuração de agendas de execução de testes e varreduras periódicos;
87. Proteção de Bots
88. Implementar proteção de tráfego volumétrico de origem automatizada em aplicações web, dispositivos móveis e APIs;
89. Deve ser totalmente integrado aos demais serviços, através da mesma console e configurações;
90. Implementar a identificação por assinatura de bots para proteção de aplicações e APIs;
91. Implementar a identificação através de análise de telemetria, indícios e evidências de automação;
92. Implementar a classificação de bots maliciosos e benignos, permitindo a resposta por classe de bot;
93. Implementar resposta para requisições suspeitas de bots;
94. Deve ser capaz de identificar scanners de vulnerabilidade, ferramentas de exploits e DoS, crawlers, spiders, assistentes de downloads, motores de buscas e de redes sociais;
95. Deve ser capaz de identificar e classificar ações automatizadas por bots maliciosos, bots benignos e usuários humanos;
96. Implementar mecanismos para detectar técnicas avançadas e sofisticadas de automação, tais como click-farms, agentes humanos, emuladores e simuladores, “macro runners” e implementar mitigação;
97. Implementar mecanismos de análises adaptativas de comportamentos e uso das aplicações e implementar mitigação;
98. Deve suportar integração com diversos fluxos da aplicação, tais como login, criação de contas, recuperação de senha, recuperação de contas, assinaturas de newsletter, entre outros;
99. Permitir classificar os fluxos protegidos de proteção, tais como login, gestão da conta, reset de senha e outros para geração de relatórios;
100. A solução não deve armazenar e processar dados pessoais, credenciais, dados digitados, payload, arquivos e informações que permitem a identificação pessoal. Será admitida a coleta e processamento do endereço IP, cabeçalhos e suas informações relacionadas, assim como o registro de utilização de teclas/caracteres;
101. Deve ser capaz de detectar e mitigar ataques de credential stuffing, account takeover, content scrapers, carding fraud, marketing fraud e inventory hoarding;
102. Deve ser capaz de detectar acesso provenientes de bots e classificar os tipos de automação utilizados;
103. Não serão aceitas soluções que dependem de CAPTCHAs para detecção e mitigação;
104. Não serão aceitas soluções que dependem principalmente de desafios em JavaScript para o navegador para detecção e mitigação;
105. Para aplicações web:
106. Permitir a inserção do código JavaScript nas páginas da aplicação;
107. Permitir especificar páginas que não devem receber a inserção do JavaScript;
108. Implementar a coleta de telemetria de aplicações web relacionados ao acesso e rede, ambiente e navegador, e ao comportamento e o modo de uso da aplicação no navegador e webview;
109. Implementar ofuscação avançada do código para prevenir técnicas de engenharia reversa;
110. Implementar atualizações/rotação do código de extração de telemetria de forma automática e frequenta para dificultar a ações de engenharia reversa;
111. Implementar técnicas contra tentativas de análises da telemetria coletados;
112. Não serão admitidas soluções que utilizam códigos JavaScript de fácil leitura e engenharia reversa;
113. Não serão admitidas soluções que utilizam telemetria coletados de fácil leitura e engenharia reversa;
114. Para aplicativos para dispositivos móveis:
115. Implementar coleta de telemetria relacionados ao acesso e rede, ambiente e dispositivo, e ao comportamento e modo de uso do aplicativo nativo para dispositivos móveis através de SDK incorporado ao aplicativo;
116. Deve ser totalmente compatível com as políticas de publicações de aplicativos das lojas Apple App Store e Google Play Store;
117. Ser compatível com aplicativos Android na versão 5.x e superior (API Level 21) e aplicativos para iOS na versão 9.x e superior;
118. Suportar frameworks estáticos e dinâmicos de aplicativos para dispositivos móveis, tais como React, Flutter, Angular e Ionic;
119. A atualização das políticas de coletas de telemetria não deve exigir a redistribuição ou atualização dos aplicativos nos dispositivos móveis;
120. Deve apresentar o resultado da análise da telemetria de forma determinística, ou seja, através de um veredito simples se se trata de tráfego automatizado, indicando, quando disponível, o motivo ou tipo de automação detectado;
121. Mitigação de ataques distribuídos de negação de serviço (ddos):
122. Implementar defesa automática de ataques de Distributed Denial-Of-Service (DDoS), protegendo continuamente todas as aplicações publicadas através do serviço avançado;
123. Deve mitigar ataques de forma transparente para a aplicação, absorvendo e bloqueando ataques;
124. Deve ser capaz de detectar ataques através da análise das taxas de requisição, erros, latência e throughput da aplicação;
125. Implementar proteção de ataques na camada de aplicação, incluindo os protocolos HTTP e DNS, incluindo, no mínimo, proteções de HTTP GET Flood, HTTP POST Flood, Slowloris e DNS Flood;
126. Implementar proteção de ataques volumétricos, incluindo SYN Flood, UDP Flood, TCP Flood e ICMP Flood;
127. Implementar proteção de ataques de negação de serviço através da exaustão de recursos ("Slow DDoS"), incluindo Slow POST e Slowloris;
128. Implementar proteção de ataques à pilha TCP;

129. Implementar proteção de ataques que utilizam falsificação de endereços IP de origem (IP spoofing);
130. Implementar detecção e mitigação automática de ataques em Camada 7 em larga escala;
131. Implementar proteção através de bloqueio geográfico;
132. Permitir criar regras de bloqueio personalizadas;
133. Permitir configurar o bloqueio de clientes com base no TLS fingerprint;
134. Permitir configurar o bloqueio de clientes com base na classificação e reputação do IP;
135. Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas por ataques web;
136. Permitir configurar o bloqueio de clientes com base no ASN do BGP;
137. Permitir configurar de mitigações específicas por aplicação;
138. Permitir configurar rate limit por aplicação;
139. Permitir configurar rate limit por usuário, onde entende-se por usuário como sendo um cliente da aplicação identificado por um IP de origem, um cookie, um cabeçalho, parâmetro da query, fingerprint TLS, geolocalização, ou combinação de alguns desses;
140. Gerenciamento e proteção de dns:
141. Implementar serviço DNS primário e secundário;
142. Implementar zona de pesquisa direta (Forward DNS Lookup Zone) e reverso (Reverse Lookup Zone);
143. Para as zonas hospedadas na solução, implementar a configuração automática de domínios e FQDN utilizados nas aplicações publicadas pela solução;
144. Possuir interface gráfica para gerenciamento de registros do DNS;
145. Implementar DNSSEC (Domain Name System Security Extensions) com gerenciamento automático de chaves;
146. Implementar proteções de ataques direcionados aos serviços de DNS;
147. Implementar proteções de ataques de DDoS;
148. Implementar a configuração de registros de DNS para funcionalidade de balanceamento de sites (Global Server Load Balancer - GSLB);
149. Implementar a verificação de disponibilidade dos sites através de testes HTTP e ICMP;
150. Implementar, pelo menos, os algoritmos de balanceamento round robin, prioridade, peso e origem;
151. Implementar persistência da resolução de nomes utilizando, pelo menos, o Local DNS da requisição;
152. Permitir configurar topologias para respostas com base em geolocalização;
153. Administração, gerenciamento e monitoramento:
154. Os serviços devem ser prestados de forma não intrusiva, ou seja, sem a necessidade de instalação de equipamentos ou softwares nas dependências da CONTRATANTE;
155. O serviço de segurança avançada deverá ser oferecido em ponto(s) de presença em território nacional;
156. As atividades de administração, gerenciamento, operação e monitoramento dos serviços deverão ser através de console web única, gráfica e central do fabricante da solução, via HTTPS com algoritmos de criptografia modernos e seguros, compatível com navegadores padrões, não sendo aceitas soluções que dependam de plugins, add-ons ou aplicação exclusiva instaladas nas estações de trabalho;
157. A console deve possuir controles de segurança, incluindo, mas não se limitando à, restrição de acesso administrativo por meio de um login seguro com autenticação de dois fatores de modo a prevenir que os serviços não sejam utilizados por terceiros não autorizados;
158. Permitir a criação de divisões administrativas de recursos através da criação de segmentos, partições, namespaces ou estrutura semelhante para agrupamento de recursos de diferentes propósitos, áreas ou finalidades da contratante, tais como "Produção", "Homologação" e "Desenvolvimento", unidade de negócio, departamento, entre outros;
159. Permitir a criação de usuários com acesso a console;
160. Permitir a utilização de provedores de identidade para autenticação e autorização de usuários sem a necessidade de importar ou sincronizar com bases externas de usuários e senhas;
161. Implementar Single Sign-On (SSO) compatível com OpenID Connect (OIDC), tais como Okta, Microsoft, Google e outros;
162. Permitir a configuração de Segundo Fator de Autenticação;
163. Permitir a criação de credenciais para acesso via API com data de expiração ou prazo de validade;
164. Permitir definir políticas de senhas, incluindo tipos de caracteres, tamanho mínimo, validade e tentativas malsucedidas;
165. Permitir a criação de grupos de usuários e associar usuários aos grupos;
166. Deve permitir a criação de perfis de acesso com diferentes níveis de acesso aos recursos da solução;
167. Dispor de diferentes perfis predefinidos com diferentes níveis de acesso para diferentes recursos da solução, incluindo acesso restrito, somente leitura, e leitura e escrita;
168. Permitir associar perfis de acesso a usuários por divisão administrativa;
169. Permitir associar perfis de acesso a grupos de usuários por divisão administrativa;
170. Implementar API REST autenticada através de tokens ou certificados para configuração de recursos, com documentação pública mantida pelo fornecedor do serviço;
171. Deve ser compatível com mTLS;
172. Dispor de um cliente de linha de comando (CLI) que implemente a API REST compatível com, pelo menos, Linux e Mac OS;
173. Possuir implementações específicas para ferramentas de automação no formato de provedores e módulos para Terraform ou coleções para Ansible;
174. Permitir a exportação de eventos para sistemas externos, incluindo logs da solução e de requisições, segurança, e auditoria das aplicações;
175. Permitir a exportação para, pelo menos, os seguintes sistemas: Kafka, Splunk, Datadog, Azure, Amazon, QRadar e servidores HTTPS genéricos;
176. Permitir a configuração de, pelo menos, 02 (dois) destinos para envio de eventos;
177. Possuir painéis online para visualização de eventos e estatísticas, incluindo, no mínimo:
178. Saúde geral da aplicação;
179. Latência fim a fim;
180. Estatísticas de TLS;
181. Eventos com origem, destino, ataque e ação;

182. Taxas de requisições, status code e métodos;
183. Latência e throughput da aplicação;
184. Total de requisições ao longo do tempo;
185. Lista de aplicações e requisições, ataques e bloqueios;
186. Tipos de eventos;
187. Ataques, origens e alvos mais comuns;
188. Assinaturas e violações mais comuns;
189. Representação gráfica das API descobertas;
190. Taxa de requisições, resposta, códigos de resposta por endpoint da API;
191. Representação gráfica de interação entre endpoints da API;
192. Métodos, endpoints e eventos de segurança;
193. Sumário de segurança;
194. Classificação de bots das requisições;
195. Volume de requisições de bots e humanos;
196. Fluxos da aplicação mais atacados por bots;
197. Lista de bots maliciosos por origem IP e tipo;
198. Informações de origem geográfica, dispositivos e plataformas relacionadas a bots;
199. Eventos de DDoS ao longo do tempo;
200. Taxa de requisições de ataques de DDoS;
201. Throughtput do DDoS;
202. Mapa geográfico indicando a origem do DDoS;
203. Origens, regiões e ASN (Autonomous System Number) mais comuns relacionadas ao ataque de DDoS;
204. Mapa geográfico das requisições de DNS por zona;
205. Gráfico de volume de requisições ao longo do tempo de DNS;
206. Lista de nomes de DNS mais solicitados;
207. Lista de tipos de requisições de DNS mais solicitadas e gráfico ao longo do tempo;
208. Gráfico de volume por tipo de resposta de DNS ao longo do tempo;
209. Possuir relatório de incidentes de segurança para investigação de ataques com agrupamento automático de eventos em incidentes;
210. Permitir a configuração de agendamento de relatórios (diários, semanais ou mensais) e enviar os resultados por e-mail para usuários específico;
211. Recursos disponíveis por unidade do serviço de proteção em nuvem:
212. Configuração de no mínimo 1 (uma) aplicação, sem limite de Servidores que originam o tráfego, onde ela deve ser configurada em um Load Balancer independente;
213. Configuração de proteção de bots com capacidade total entre todas as aplicações (web e móvel) de analisar 500.000 (quinhentas mil) de transações por dia, 24x7, todos os dias do ano;
214. Proteger com regras de WAF com capacidade de tratar no mínimo 5 (cinco) milhões de transações/mês;
215. Entende-se por aplicação como a configuração de um FQDN ou domínio que deve ser protegido por uma política de segurança, acessível por um IP ou CNAME, independente da quantidade de paths ou URL deste FQDN;
216. Capacidade de limitar taxas de requisições válidas (rate limit) de usuários identificados de, no mínimo, 10.000.000,00 (dez milhões) requisições/mês entre todas as aplicações;
217. Capacidade de realizar testes de vulnerabilidades para 03 (três) aplicações/mês;
218. Capacidade de mitigar DDoS independente do volume de tráfego, sem custo adicional;
219. Serviço de DNS autoritativo primário e secundário para, no mínimo, 150 (cento e cinquenta) zonas, sem limite de resoluções e resposta de DNS;
220. Serviço de balanceamento de DNS para, pelo menos 30 (trinta) endereços IP;
221. Garantir via console o acesso, busca e consulta de eventos por, no mínimo:
222. 30 (trinta) dias para métricas de desempenho e eventos de auditoria;
223. (sete) dias para eventos de requisições e segurança.

7.2.5. A solução de Firewall de Aplicação Web (WAF) e Solução de Segurança Avançada deverá contemplar mecanismos de **backup automático** de todas as configurações críticas do ambiente, incluindo, no mínimo: políticas de segurança, regras de balanceamento, perfis de acesso, certificados digitais, registros de auditoria e demais parâmetros operacionais relevantes, devendo ser possível:

1. Agendar rotinas de backup automático em periodicidade definida pela CONTRATANTE (diária, semanal e mensal), sem interrupção dos serviços em produção.
2. Armazenar os arquivos de backup em repositório local e/ou remoto indicado pela CONTRATANTE, com suporte a transmissão segura (ex.: SCP, SFTP, HTTPS) e criptografia dos dados em repouso e em trânsito.
3. Manter política de retenção configurável, permitindo a definição de quantidade mínima de versões de backup e prazo de armazenamento, em observância às normas internas de segurança da informação e à legislação aplicável.
4. Realizar o restabelecimento (restore) completo ou parcial da configuração a partir de qualquer ponto de backup disponível, com trilha de auditoria das operações de backup e restauração (data, hora, usuário responsável e elementos restaurados).
5. Permitir que o procedimento de backup e restauração seja documentado e validado durante a implantação, com realização de testes práticos e registro em relatório técnico, a fim de assegurar a continuidade dos serviços em caso de falhas, incidentes de segurança ou necessidade de recuperação de ambiente.

7.2.6. O atendimento a este requisito é condição essencial para a elevação da postura de segurança, continuidade dos serviços educacionais e conformidade com a Política de Segurança da Informação do Governo do Estado de Rondônia

7.3. **Forma de execução do objeto:**

7.3.1. A execução do objeto será realizada de forma estruturada, em etapas claramente definidas, visando garantir a eficiência, a segurança, a rastreabilidade

e a conformidade com os requisitos técnicos, legais e normativos. O processo de execução abrange as fases de entrega, integração, acompanhamento, fiscalização e recebimento dos equipamentos e serviços, conforme previsto no art. 40 da Lei nº 14.133/2021 e no art. 13 da IN SEGES nº 58/2022.

7.3.2. A entrega dos equipamentos deverá ser realizada no endereço indicado pela Administração, em lotes, conforme cronograma pactuado, acompanhados de nota fiscal, termo de garantia, documentação técnica e certificados de conformidade. A entrega será precedida de comunicação formal e deverá observar os requisitos de segurança e integridade dos equipamentos, incluindo embalagem adequada, transporte seguro e identificação clara dos volumes. A conferência dos equipamentos será realizada por equipe designada, utilizando checklists de conformidade e sistemas de registro de ocorrências, garantindo a rastreabilidade e a transparência do processo.

7.3.3. Os bens deverão ser entregues à Coordenadoria de Almoxarifado e Patrimônio (SEDUC-CAP), que é responsável, dentre outros, pelo armazenamento, controle de estoque e distribuição dos materiais à destinação final. As entregas dos equipamentos deverão ser efetuadas mediante prévio agendamento junto a SEDUC-CAP, no seguinte local:

Endereço: Rua Uruguai, nº 3457, Bairro Industrial, CEP: 76.821-010, em Porto Velho - RO.

Horário de atendimento: segunda à sexta-feira, no horário das 07h30 às 13h30.

Telefone: (69) 3212-8215 e (69) 3212-8216 - Gerente de Apoio, Logística e Distribuição (SEDUC-GALD/CAP).

E-mail: gald@seduc.ro.gov.br

7.3.4. Os serviços e softwares deverão ser entregues à **Gerência de Segurança da Informação e Operação de Redes - GSIOR**, que é responsável pela contratação, gerência e fiscalização do objeto, no seguinte local:

Endereço SEDUC: Av. Farquar, 2986 - Bairro Pedrinhas

Palácio Rio Madeira - Edifício Rio Guaporé, 3º andar, Porto Velho, RO, CEP 76801470

Horário de atendimento: segunda à sexta-feira, no horário das 07h30 às 13h30.

Telefone: (69) 3212-8253 - SEDUC-GSIOR.

E-mail: gsior@seduc.ro.gov.br

7.3.5. A integração dos equipamentos à infraestrutura existente será realizada por profissionais qualificados, sob supervisão da equipe de TIC da instituição.

7.3.6. Essa etapa inclui a instalação física dos equipamentos, configuração inicial, atualização de firmware e software, testes de funcionamento, validação de compatibilidade com sistemas legados e aplicação de políticas de segurança da informação. A integração deverá observar os padrões definidos no ETP, na arquitetura institucional de TIC e nas normas técnicas aplicáveis, garantindo a interoperabilidade, a escalabilidade e a aderência aos requisitos de desempenho e segurança.

7.3.7. O acompanhamento e a fiscalização da execução contratual serão exercidos por equipe designada, composta por servidores da área de TIC e representantes das áreas usuárias, conforme art. 117 da Lei nº 14.133/2021. A fiscalização será realizada por meio de inspeções técnicas, validação de funcionalidades, verificação de aderência às especificações, análise de relatórios de acompanhamento e aplicação de indicadores de desempenho. Serão utilizados sistemas informatizados para registro de ocorrências, controle de prazos, gestão de chamados e geração de relatórios gerenciais, promovendo a transparência, a eficiência e a prestação de contas.

7.3.8. O recebimento provisório dos equipamentos ocorrerá após a entrega e instalação, mediante verificação quantitativa e qualitativa, conferência de documentação e realização de testes de funcionamento. O recebimento definitivo será realizado após período de testes e validação, conforme art. 140 da Lei nº 14.133/2021, mediante termo circunstanciado, assegurando que todos os requisitos contratuais foram atendidos. Eventuais não conformidades deverão ser registradas e comunicadas ao fornecedor para correção, dentro dos prazos estabelecidos em contrato.

7.3.9. Todo o processo de execução será documentado em sistema próprio, garantindo a rastreabilidade, a transparência e a conformidade com os princípios da administração pública, em especial a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência.

7.4. **Definição de nível mínimo de serviço**

7.5. A contratada deverá garantir a prestação contínua dos serviços, respeitando os seguintes parâmetros mínimos de desempenho e qualidade:

7.5.1. **Atendimento Técnico e Suporte**

- Atendimento presencial ou remoto, conforme necessidade da CONTRATANTE, com suporte técnico tipo 8x5 (oito horas diárias, cinco dias por semana) e operação 24x7 para ambientes críticos.
- Atendimento ilimitado para abertura de chamados técnicos.

7.5.2. **Classificação das Ocorrências**

7.5.2.1. Os chamados serão classificados conforme a severidade da ocorrência, observando os prazos máximos para atendimento e solução/paliativo:

Severidade	Condição	Atendimento	Solução/Paliativo
Alta	Indisponibilidade total de funcionalidade crítica da solução	4 horas	12 horas
Média	Falhas com impacto parcial (instabilidade, lentidão)	6 horas	24 horas
Baixa	Dúvidas, ajustes de configuração ou manutenção preventiva	24 horas	48 horas
Locais Remotos	Paralisação total em ambientes de difícil acesso (ex: interior, zona rural)	96 horas	120 horas

- O tempo será contado a partir da abertura do chamado.
- Chamados só poderão ser encerrados mediante anuência da CONTRATANTE.

7.5.3. O estabelecimento do Nível Mínimo de Serviço – NMS mostra-se aplicável à presente contratação em razão da criticidade da solução de segurança da informação e da necessidade de assegurar continuidade, disponibilidade e capacidade de resposta adequada a incidentes que possam comprometer as aplicações e os ativos tecnológicos da SEDUC-RO.

7.5.4. As métricas estabelecidas no item 7.4. foram definidas com base na classificação da severidade dos eventos e na correspondente necessidade de resposta da CONTRATADA, mediante definição objetiva de prazos para atendimento e solução, permitindo à Administração aferir o desempenho contratual e aplicar, quando cabível, as medidas previstas no instrumento contratual.

7.5.5. A adoção dessas métricas mostra-se adequada à natureza do objeto, que compreende, além do fornecimento dos appliances e respectivas licenças, serviços de suporte técnico e solução de segurança em nuvem, cuja continuidade e disponibilidade são essenciais à manutenção da proteção das aplicações institucionais.

7.5.6. **Monitoramento e Operação Assistida**

7.5.6.1. A solução deverá dispor de recursos de observabilidade e monitoramento contínuo, com emissão de alertas automáticos e geração de logs de eventos.

7.5.6.2. Durante o período de operação assistida, após o término da instalação e configuração da solução, deverá haver alocação de profissional certificado pelo

fabricante da solução para atuação nas dependências da CONTRATANTE por ao menos 2 (duas) semanas.

7.5.6.3. O profissional, com o apoio de sua equipe remota, deverá integrar, monitorar e documentar pelo menos 500 dispositivos/elementos de rede na plataforma de observabilidade. Caso não existam mais atividades que necessitem da disponibilidade presencial do profissional, elas poderão continuar a serem executadas remotamente.

7.5.6.4. Serão realizadas atividades de capacitação técnica e apoio à manutenção corretiva e preventiva.

7.5.7. **Relatórios de Atendimento e Monitoramento**

7.5.7.1. A contratada deverá fornecer mensalmente, até o 5º dia útil do mês subsequente relatório analítico e sintético com:

- Total de chamados por severidade;
- Tempo de atendimento e solução;
- Descrição das ocorrências e soluções aplicadas;
- Indicadores de desempenho da plataforma;
- Análise de tendências e sugestões de melhoria.

7.5.8. **Requisitos de Manutenção e Garantia**

- Todas as atualizações, correções de falhas (patches), releases e upgrades das licenças fornecidas deverão estar incluídas.
- Eventuais interrupções programadas devem ser previamente comunicadas à CONTRATANTE com no mínimo 24 horas de antecedência.
- A contratada será responsável por manter a estabilidade da solução e assegurar sua plena funcionalidade durante toda a vigência contratual.

7.5.9. **Segurança da Informação**

7.5.9.1. A contratada deverá atender às normas e diretrizes da Política de Segurança da Informação (PSI) da SETIC/RO, conforme Portaria nº 97/2021, assegurando:

- Proteção contra vazamentos de dados;
- Controle de acesso;
- Registro e rastreabilidade de eventos;
- Cumprimento das diretrizes de privacidade da informação institucional.

7.6. **Descrição da Arquitetura Tecnológica**

7.6.1. A arquitetura tecnológica proposta é composta por um cluster de dois equipamentos físicos (appliances) de Firewall de Aplicações Web (WAF), em alta disponibilidade (HA), posicionados na borda da rede da SEDUC-RO, integrados aos ambientes de rede IP/MPLS e à INFOVIA do Estado.

7.6.2. Essa solução realiza inspeção profunda de tráfego na camada de aplicação (L7), suporta múltiplos domínios de roteamento, implementa balanceamento de carga, DNS seguro, integração com plataformas de virtualização e orquestração de containers (Kubernetes/OpenShift), além de prover visibilidade, controle e mitigação em tempo real de ameaças via telemetria, inteligência artificial e assinaturas atualizadas automaticamente.

7.7. **Plano de Transferência de Conhecimento**

7.7.1. Para garantir a autonomia da equipe interna da SEDUC-RO na operação da solução contratada, o fornecedor deverá apresentar e executar um plano de transferência de conhecimento, contendo no mínimo:

- Treinamento técnico com conteúdo técnico-operacional na solução ofertada para 10 (dez) servidores – cada unidade adquirida deste serviço compreende a um treinamento para 1 (um) aluno; com carga horária mínima de 40 horas, executado de modo remoto e síncrono;
- Conteúdo programático incluindo administração, segurança, operação, diagnóstico e atualização da solução;
- Material didático em português e acesso à base de conhecimento online do fabricante;
- Simulações práticas e laboratórios de operação, na própria solução fornecida;
- Certificação de conclusão para todos os participantes;
- Suporte técnico consultivo nos primeiros 90 dias após entrega técnica para acompanhamento da curva de aprendizagem.

7.8. **Detalhamento da Documentação da Solução**

7.8.1. A documentação a ser entregue deverá contemplar:

- Guia de instalação física e lógica;
- Manual de configuração detalhado, com perfis e políticas aplicadas;
- Plano de endereçamento IP e VLANs utilizados na integração;
- Topologia de rede implementada (diagrama lógico e físico);
- Procedimentos de backup e restauração de configurações;
- Inventário técnico dos equipamentos e licenças;
- Relatório de testes de aceitação e desempenho da solução;
- Procedimentos de troubleshooting e recuperação de falhas;
- Registro das sessões de treinamento com listas de presença;
- Políticas de segurança implementadas, incluindo OWASP Top 10, DDoS, WAF e API Security.

7.8.2. Toda a documentação deverá estar em formato digital (PDF e editável) e ser entregue até o prazo de aceite definitivo da solução.

7.9. **Garantia do produto**

7.9.1. Considerando a natureza do objeto, a garantia desta contratação será de, 60 (sessenta) meses contados a partir da data de recebimento definitivo, prevalecendo a garantia oferecida pelo fabricante se o prazo for superior, devendo o licitante arrematante informar em sua proposta ou anexo o prazo de garantia ofertado;

7.9.2. A garantia do produto, no prazo mínimo estipulado no item anterior, não desonera a Contratada de cumprir as obrigações previstas na Lei nº 8.078 de 11/09/90, e alterações – Código de Defesa do Consumidor, bem como dos encargos previstos neste instrumento.

7.9.3. Sendo evidenciado defeito em prazo igual ou inferior a 7 (sete) dias corridos, o bem deverá ser substituído pelo contratado, no prazo de até 15 (quinze)

dias corridos, por outro bem, novo, sem uso.

7.9.4. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

7.9.5. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

7.9.6. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

7.9.7. Durante o **PERÍODO DE GARANTIA** e em caso de necessidade de substituição de equipamentos/acessório ou peças que não mais existam no mercado, ou que estejam fora de linha de fabricação em razão de evolução tecnológica ou que, por qualquer outro motivo o fabricante não mais o produza, e, caso assim aconteça, de manter a oferta de componentes e peças de reposição por período razoável de tempo, nunca inferior à vida útil do produto ou serviço, a proceder a substituição por produto e/ou componente tecnologicamente equivalente ou superior.

7.10. **Critérios para Medição de Demandas e Governança de TIC**

7.10.1. A governança da solução será orientada por indicadores objetivos e auditáveis, conforme diretrizes da Instrução Normativa SGD/ME nº 1/2019 e boas práticas de governança de TIC. Os critérios de medição de demandas incluirão:

- Volume de requisições e transações por segundo processadas;
- Relatórios mensais de incidentes e violações detectadas;
- Número de regras e políticas configuradas/ajustadas mensalmente;
- Análises periódicas de desempenho e de logs exportados para SIEM;
- Uso da base de inteligência de ameaças, atualizações e métricas correlatas;
- Número de eventos mitigados por tipo de ataque (DoS, SQLi, XSS, etc.);
- Adesão às políticas de segurança e conformidade com a PSI da SETIC-RO (0063003489).

7.10.2. Além disso, será instituído um comitê de acompanhamento com representantes da COTIC/SEDUC e da contratada, que se reunirá trimestralmente para:

- Exame de Conformidade/ Prova Conceito facultativoAvaliar o cumprimento contratual;
- Ajustar parâmetros de operação;
- Planejar evoluções tecnológicas e atualizações;
- Avaliar novos riscos e propor planos de mitigação.

7.10.3. A métrica de medição adotada para a presente contratação considera as características efetivas do objeto, composto pelo fornecimento de equipamentos (appliances), respectivas licenças, implantação e configuração, serviços de suporte e manutenção e solução de segurança em nuvem.

7.10.4. Dessa forma, a aferição da execução contratual não se baseia em volume de desenvolvimento ou produção de funcionalidades de software, mas no cumprimento das obrigações e dos níveis de serviço estabelecidos, considerando, conforme aplicável, a disponibilidade da solução, a classificação dos incidentes, os prazos de atendimento e solução, o cumprimento dos requisitos técnicos e demais resultados objetivamente previstos neste Termo de Referência.

7.10.5. A métrica adotada permite à Administração verificar objetivamente o desempenho da CONTRATADA, especialmente quanto à continuidade e à qualidade dos serviços de suporte e da solução de segurança, bem como subsidiar o aceite, a aplicação de eventuais glosas e a avaliação do cumprimento das obrigações contratuais.

7.10.6. A escolha dessa metodologia decorre, portanto, da própria natureza do objeto, que não envolve desenvolvimento de sistemas sob demanda ou execução de atividades cuja dimensão possa ser adequadamente mensurada pela quantidade de funcionalidades desenvolvidas, mas sim o fornecimento e a operação assistida de solução tecnológica de segurança da informação com requisitos técnicos, níveis de serviço e resultados previamente definidos.

7.11. **Da Participação de Sociedades Cooperativas**

Para a presente contratação **será admitido** a contratação de Sociedade Cooperativa, em função da natureza do serviço demandar subordinação entre a cooperativa e os cooperados e os cooperados e a administração.

7.12. **Do Consórcio:**

7.12.1. Tendo em vista que, é prerrogativa do Poder Público, na condição de contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme se depreende da literalidade do texto da Lei Nº 14.133/21 e ainda o entendimento do Acórdão TCU nº 1316/2010, que atribui à Administração a prerrogativa de admissão de consórcios em licitações por ela promovidas:

7.12.2. Fica vedada a participação de empresas em consórcio, tendo em vista que o objeto a ser licitado não envolve questões de alta complexidade técnica, operacional ou econômica que impeça, isoladamente, a prestação do **serviço de fornecimento de solução de equipamentos Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, dos ativos de hardware e software e das aplicações Web**, ao ponto de haver necessidade de parcelamento do objeto, através da união de esforços.

7.12.3. A justificativa acerca da não participação de empresas enquadradas nas modalidades de Consórcio e Cooperativa no presente procedimento licitatório.

Acerca dos Consórcios esta SEDUC, informa que a conveniência de admitir a participação dos mesmos em procedimento licitatório é decisão meramente discricionária da Administração, art. 15, da Lei nº 14.133/2021.

7.12.4. Sobre o tema, Marçal Justen Filho (Comentários à lei de licitações e contratos administrativos, 12. ed., São Paulo: Dialética, p. 410) assevera:

> O ato convocatório admitirá ou não a participação de empresas em consórcio. Trata-se de escolha discricionária da Administração Pública, o que evidentemente não significa autorização para decisões arbitrárias ou imotivadas.

7.12.5. E assim conclui:

Admitir ou negar a participação de consórcios é o resultado de um processo de avaliação do mercado em face do objeto a ser licitado e da ponderação dos riscos inerentes à atuação de uma pluralidade de sujeitos associados para a execução do objeto.

Dessa forma, não seria vantajoso para a Administração Pública contratar empresas em regime de consórcio, tendo em vista que estas empresas passariam a ter responsabilidade solidária no que concerne às obrigações trabalhistas e previdenciárias, o que traria riscos para a contratação, podendo gerar graves repercussões para o cumprimento do contrato celebrado com o Estado, caso tal empresa, de repente, tivesse os seus valores financeiros bloqueados pela Justiça, para fins de pagamento de dívidas.

A vedação quanto à participação de consórcio de empresas no presente procedimento licitatório não limitará a competitividade.

7.13. **Prazo de Assinatura do Contrato:**

7.13.0.1. O contrato deverá ser assinado, em até **03 (três) dias** úteis a \contar da convocação.

7.13.0.2. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação da parte durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração, na forma do art. 90, § 1º da Lei 14.133/2021.

8. CONDIÇÕES DE EXECUÇÃO:

8.1. A execução do objeto seguirá a seguinte dinâmica:

8.1.1. O contrato será fielmente executado pelas partes nos termos do art. 115 da Lei nº 14.133/2021.

8.1.2. 15 dias para licenças de software e/ou serviços, caso o licenciamento dependa de algum equipamento físico para a sua correta execução, admitir-se-á o prazo de fornecimento idêntico ao do equipamento para o início das execuções de serviço;

8.1.3. Início da execução do objeto: 05 (cinco) dias, após o recebimento da emissão da ordem de serviço;

8.1.4. Prazo de 30 (trinta) dias para conclusão do serviço.

8.2. Os equipamentos serão aceitos após confecção visual, verificação de marca e modelo contratados e apontamento de número de série.

8.3. Os serviços serão aceitos após a instalação dos equipamentos nos locais determinados e a conexão lógica dos equipamentos com as suas respectivas controladoras seguras.

8.4. Somente será possível a prorrogação do prazo de entrega, mediante o cumprimento, pela Contratada, dos seguintes requisitos cumulativos:

a) Solicitação de prorrogação protocolada dentro do prazo de entrega dos materiais/bens;

b) Comprovação documental da ocorrência de motivo imprevisível (caso fortuito, força maior ou fato do príncipe), ocorrido depois da apresentação de sua proposta, que tenha correlação direta de causa e efeito sobre a necessidade do atraso.

8.5. Não se admitirá prorrogação se:

a) O atraso ocorrer por culpa da contratada;

b) Se não cumprir os requisitos elencados quanto ao prazo de entrega.

c) Houver interesse público devidamente justificado nos autos que demonstre ser a escolha mais vantajosa para a administração.

8.6. Ocorrendo recusa ou atraso na entrega total ou parcial do bem, o responsável pela fiscalização do contrato se obriga por força do Art. 4º da Lei Estadual nº. 2.414/11, a produzir parecer técnico e o encaminhará ao ordenador de despesas para instauração de procedimento administrativo, instrução dos autos para fins de penalização da contratada e inserção no "*Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual*".

8.7. Qualquer solicitação de informações complementares e outros assuntos relacionados a esta contratação deverão ser tratados junto a Coordenadoria de Tecnologia da Informação e Comunicação - COTIC, de segunda-feira à sexta-feira, no horário de 08:00hs às 13:30hs.

8.8. O recebimento dos materiais se dará da seguinte forma:

a) **provisoriamente,** de forma sumária, pelo responsável por seu acompanhamento e fiscalização, com verificação posterior da conformidade do material com as exigências contratuais;

b) **definitivamente,** por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

8.9. Os prazos e os métodos para a realização dos recebimentos provisório e definitivo serão definidos em regulamento ou no contrato.

8.10. No ato do recebimento, caso o material apresentado não estiver em conformidade com as especificações constantes no Termo de Referência, o item será recusado total ou parcialmente conforme o caso, sem direito a indenização à empresa vencedora.

8.11. Caso se verifique que não se mostra possível a adequação do objeto deste estudo ou que não foi alcançado o resultado esperado, será cabível a extinção do Contrato, com base no que dispõe o art. 137 e incisos, da Lei nº 14.133/21 assegurados o contraditório e a ampla defesa, bem como a aplicação de penalidades, conforme o disposto no art. 156, parágrafos 4º e 5º da referida Lei.

8.12. O objeto desta contratação deverá estar acompanhado de nota fiscal com o nome e caracterização clara e precisa dos produtos. Deverá conter o número da Nota de Empenho.

9. MODELO DE GESTÃO DE CONTRATOS:

9.1. 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.

9.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato quanto a fase de elaboração de projetos e execução da obra/adaptação, o cronograma de execução poderá ser prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

9.3. 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.

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

9.5. 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.

9.6. Preposto:

9.6.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

9.6.2. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

9.7. Fiscalização:

9.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo (s) fiscal (is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

9.8. Fiscalização Técnica:

9.8.1. 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. (Lei nº 14.133, de 2021, art. 117, §1º e art. 23, II do Dec. Estadual nº 28.874/2028.

9.8.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 28.874/2024, art. 23, III);

9.8.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 28.874/2024, art. 23, III);

9.8.4. O fiscal técnico do contrato comunicará imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas; (Decreto Estadual nº 28.874/2024, art. 23, V);

9.8.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto Estadual nº 28.874/2024, art. 23, V).

9.8.6. Durante a execução do objeto, fase do recebimento provisório, o fiscal técnico designado deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à contratada a correção das faltas, falhas e irregularidades constatadas.

9.8.7. O fiscal técnico do contrato deverá apresentar ao preposto da contratada a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

9.8.8. O preposto deverá apor assinatura no documento, tomando ciência da avaliação realizada.

9.8.9. A contratada poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

9.8.10. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à contratada de acordo com as regras previstas no ato convocatório.

9.8.11. É vedada a atribuição à contratada da avaliação de desempenho e qualidade da prestação dos serviços por ela realizada.

9.8.12. O fiscal técnico poderá realizar a avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

9.8.13. A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos na Lei n. 14.133/2021. (IN05/17 - art. 62)

9.8.14. A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada destes, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso. (art. 47, §2º, IN 05/2017)

9.8.15. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da Contratada, 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 da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

9.8.16. 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.

9.8.17. Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal técnico do contrato deverá 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 no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

9.9. **Fiscalização Administrativa:**

9.9.1. O fiscal administrativo do contrato certificar-se de que a contratada mantém, durante toda execução do contrato, as condições de habilitação e qualificação exigidas na licitação e/ou na contratação, solicitando os documentos necessários a esta constatação.

9.9.2. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto Estadual nº 28.874/2024, art. 24, IV).

9.9.3. A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

9.9.4. Na fiscalização do cumprimento das obrigações trabalhistas e sociais exigir-se-á, dentre outras, as seguintes comprovações:

9.9.4.1. No caso de empresas regidas pela Consolidação das Leis do Trabalho (CLT):

no primeiro mês da prestação dos serviços, a contratada deverá apresentar a seguinte documentação:

a) relação dos empregados, contendo nome completo, cargo ou função, horário do posto de trabalho, números da carteira de identidade (RG) e da inscrição no Cadastro de Pessoas Físicas (CPF), com indicação dos responsáveis técnicos pela execução dos serviços, quando for o caso;

b) Carteira de Trabalho e Previdência Social (CTPS) dos empregados admitidos e dos responsáveis técnicos pela execução dos serviços, quando for o caso, devidamente assinada pela contratada;

c) exames médicos admissionais dos empregados da contratada que prestarão os serviços; e

d) entrega até o dia trinta do mês seguinte ao da prestação dos serviços ao setor responsável pela fiscalização do contrato dos seguintes documentos, quando não for possível a verificação da regularidade destes no Sistema de Cadastro de Fornecedores (Sicaf):

- Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND);
- certidões que comprovem a regularidade perante as Fazendas Estadual, Distrital e Municipal do domicílio ou sede do contratado;
- Certidão de Regularidade do FGTS (CRF); e
- Certidão Negativa de Débitos Trabalhistas (CNDT).

9.9.5. Entrega, quando solicitado pelo Contratante, de quaisquer dos seguintes documentos:

- extrato da conta do INSS e do FGTS de qualquer empregado, a critério da Administração contratante;
- cópia da folha de pagamento analítica de qualquer mês da prestação dos serviços, em que conste como tomador a parte contratante;
- cópia dos contracheques dos empregados relativos a qualquer mês da prestação dos serviços ou, ainda, quando necessário, cópia de recibos de depósitos bancários;
- comprovantes de entrega de benefícios suplementares (vale-transporte, vale-alimentação, entre outros), a que estiver obrigada por força de lei ou de Convenção ou Acordo Coletivo de Trabalho, relativos a qualquer mês da prestação dos serviços e de qualquer empregado; e
- comprovantes de realização de eventuais cursos de treinamento e reciclagem que forem exigidos por lei ou pelo contrato.

9.9.6. Entrega de cópia da documentação abaixo relacionada, quando da extinção ou rescisão do contrato, após o último mês de prestação dos serviços, no prazo definido no contrato:

- termos de rescisão dos contratos de trabalho dos empregados prestadores de serviço, devidamente homologados, quando exigível pelo sindicato da categoria;

- guias de recolhimento da contribuição previdenciária e do FGTS, referentes às rescisões contratuais;
- extratos dos depósitos efetuados nas contas vinculadas individuais do FGTS de cada empregado dispensado;
- exames médicos demissionais dos empregados dispensados.

9.9.7. Sempre que houver admissão de novos empregados pela contratada, os documentos elencados no item 9.9.4.1 acima deverão ser apresentados.

9.9.8. A Administração deverá analisar a documentação solicitada no item 9.9.4. acima no prazo de 30 (trinta) dias após o recebimento dos documentos, prorrogáveis por mais 30 (trinta) dias, justificadamente.

9.9.9. A cada período de 12 meses de vigência do contrato de trabalho, a contratada deverá encaminhar termo de quitação anual das obrigações trabalhistas, na forma do art. 507-B da CLT, ou comprovar a adoção de providências voltadas à sua obtenção, relativamente aos empregados alocados, em dedicação exclusiva, na prestação de serviços contratados.

9.9.10. O termo de quitação anual efetivado deverá ser firmado junto ao respectivo Sindicato dos Empregados e obedecerá ao disposto no art. 507-B, parágrafo único, da CLT.

9.9.11. Para fins de comprovação da adoção das providências a que se refere o presente item, será aceito qualquer meio de prova, tais como: recibo de convocação, declaração de negativa de negociação, ata de negociação, dentre outros.

9.9.12. Não haverá pagamento adicional pela Contratante à Contratada em razão do cumprimento das obrigações previstas neste item.

9.9.13. No caso de sociedades diversas, tais como as Organizações Sociais Civis de Interesse Público (Oscip's) e as Organizações Sociais, será exigida a comprovação de atendimento a eventuais obrigações decorrentes da legislação que rege as respectivas organizações.

9.9.14. Os documentos necessários à comprovação do cumprimento das obrigações sociais trabalhistas poderão ser apresentados em original ou por qualquer processo de cópia autenticada por cartório competente ou por servidor da Administração.

9.9.15. Em caso de indício de irregularidade no recolhimento das contribuições previdenciárias, os fiscais ou gestores de contratos de serviços com regime de dedicação exclusiva de mão de obra deverão oficiar à Receita Federal do Brasil (RFB).

9.9.16. Em caso de indício de irregularidade no recolhimento da contribuição para o FGTS, os fiscais ou gestores de contratos de serviços com regime de dedicação exclusiva de mão de obra deverão oficiar ao Ministério do Trabalho.

9.9.17. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pelo contratado poderá dar ensejo à rescisão contratual, sem prejuízo das demais sanções.

9.9.18. A Administração contratante poderá conceder um prazo para que a contratada regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade da empresa de corrigir.

9.9.19. Caso não seja apresentada a documentação comprobatória do cumprimento das obrigações trabalhistas, previdenciárias e para com o FGTS, a CONTRATANTE comunicará o fato à CONTRATADA e reterá o pagamento da fatura mensal, em valor proporcional ao inadimplemento, até que a situação seja regularizada.

9.9.20. Não havendo quitação das obrigações por parte da Contratada no prazo de quinze dias, a Contratante poderá efetuar o pagamento das obrigações diretamente aos empregados da contratada que tenham participado da execução dos serviços objeto do contrato.

9.9.21. O sindicato representante da categoria do trabalhador deverá ser notificado pela Contratante para acompanhar o pagamento das verbas mencionadas.

9.9.22. Tais pagamentos não configuram vínculo empregatício ou implicam a assunção de responsabilidade por quaisquer obrigações dele decorrentes entre a contratante e os empregados da Contratada.

9.9.23. O contrato só será considerado integralmente cumprido após a comprovação, pela Contratada, do pagamento de todas as obrigações trabalhistas, sociais e previdenciárias e para com o FGTS referentes à mão de obra alocada em sua execução, inclusive quanto às verbas rescisórias.

9.9.24. A Contratada é responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

9.9.25. A inadimplência da Contratada, com referência aos encargos trabalhistas, fiscais e comerciais não transfere à Administração Pública a responsabilidade por seu pagamento.

9.9.26. A fiscalização administrativa observará, ainda, as diretrizes relacionadas no item 10 do Anexo VIII-B da Instrução Normativa nº 5, de 26 de maio de 2017, cuja incidência se admite por força da Instrução Normativa Seges/Me nº 98, de 26 de dezembro de 2022.

9.9.27. Para efeito de recebimento provisório, ao final de cada período mensal, o fiscal administrativo deverá verificar a efetiva realização dos dispêndios concernentes aos salários e às obrigações trabalhistas, previdenciárias e com o FGTS do mês anterior, dentre outros, emitindo relatório que será encaminhado ao gestor do contrato.

9.10. **Fiscalização Setorial:**

9.10.1. Para efeito de recebimento provisório, ao final de cada período mensal, caberá ao fiscal setorial do contrato e nos seus impedimentos legais, ao seu substituto, exercer as atribuições de que tratam a fiscalização Técnica e Administrativa, retro descritas.

9.11. **Gestor do Contrato:**

9.11.1. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

9.11.2. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

9.11.3. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial 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.

9.11.4. O gestor do contrato tomará 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 Federal nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso (Decreto Estadual nº 28.874/2024 art. 20, XV).

9.11.5. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto Estadual nº 28.874/2024 art. 20, XIV).

9.11.6. receber as notas fiscais atestadas pelo(s) fiscal(is) do contrato e encaminhá-las para o setor responsável pelo pagamento, após conferência dos respectivos documentos (Decreto Estadual nº 28.874/2024 art. 20, IX).

9.11.7. O gestor do contrato deverá 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.

10. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO:

10.1. **Do regime de execução, medição e pagamento**

10.1.1. A execução contratual observará regime diferenciado de acordo com a natureza das parcelas que compõem o objeto, distinguindo-se os componentes de fornecimento e implantação, de execução pontual, dos serviços de natureza continuada.

10.1.2. O fornecimento dos appliances, respectivas licenças e demais componentes de entrega pontual será executado mediante o cumprimento dos marcos de entrega, implantação e aceite estabelecidos neste Termo de Referência, sendo o pagamento correspondente realizado após o recebimento e aceite pela Administração, observados os requisitos técnicos e documentais aplicáveis.

10.1.3. A instalação e configuração dos appliances serão consideradas concluídas somente após a execução das atividades previstas, realização dos testes de funcionamento, integração ao ambiente da SEDUC-RO e emissão do respectivo aceite técnico pela fiscalização contratual.

10.1.4. Os serviços de suporte técnico, manutenção e a Solução de Segurança Avançada serão prestados de forma continuada pelo período de 60 (sessenta) meses, sendo sua medição e pagamento realizados mensalmente, condicionados à efetiva prestação dos serviços e ao cumprimento dos níveis mínimos de serviço estabelecidos neste Termo de Referência.

10.1.5. A medição mensal dos serviços continuados considerará, no mínimo, o cumprimento dos níveis mínimos de serviço, os prazos de atendimento e solução dos chamados, a disponibilidade da solução e os demais indicadores de desempenho estabelecidos neste Termo de Referência.

10.1.6. O pagamento mensal ficará condicionado ao aceite da medição pela fiscalização contratual, mediante ateste da efetiva prestação dos serviços, sem prejuízo da aplicação das glosas decorrentes do descumprimento dos níveis mínimos de serviço ou de outras obrigações mensuráveis previstas neste Termo de Referência.

10.1.7. As glosas serão aplicadas de forma proporcional ao inadimplemento verificado, observados os critérios, indicadores, metas e percentuais estabelecidos no instrumento de medição e nos níveis mínimos de serviço, sem prejuízo da aplicação das sanções administrativas cabíveis quando configurada infração contratual.

10.1.8. O aceite dos componentes de entrega pontual não implica, por si só, o aceite dos serviços continuados, cuja execução será aferida mensalmente durante o período contratual de 60 (sessenta) meses.

10.1.9. O reajustamento dos preços observará a legislação aplicável e a periodicidade estabelecida no instrumento contratual. Para as parcelas relativas aos serviços continuados, será utilizado o Índice de Custo da Tecnologia da Informação – ICTI, divulgado pelo Instituto de Pesquisa Econômica Aplicada – IPEA, como índice de referência para o reajustamento, observado o disposto no art. 25, § 7º, da Lei Federal nº 14.133/2021 e as demais condições previstas no contrato.

10.1.10. O reajustamento não incidirá sobre parcelas de execução pontual que já tenham sido integralmente entregues, recebidas e pagas pela Administração, restringindo-se às parcelas sujeitas à incidência do reajuste, na forma estabelecida no instrumento contratual.

10.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

- não produzir os resultados acordados;
- deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou,
- deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

10.3. **Do Recebimento:**

10.3.1. Os serviços serão recebidos provisoriamente, no prazo de até 5 (cinco) dias, pelos fiscais técnico, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 23, X e Art. 24, VII do Decreto Estadual nº 28.874, de 2024).

10.3.2. 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.

10.3.3. 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. (Art. 23, X, Decreto Estadual nº 28.874, de 2024).

10.3.4. 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. (Art. 24, VII, Decreto Estadual nº 28.874, de 2024).

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

10.3.6. Para efeito de recebimento provisório, ao final de cada período mensal:

- o fiscal técnico do contrato deverá 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 no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;
- o fiscal administrativo deverá verificar a efetiva realização dos dispêndios concernentes aos salários e às obrigações trabalhistas, fiscais, previdenciárias e com o FGTS do mês anterior, dentre outros, emitindo relatório que será encaminhado ao gestor do contrato.

10.3.7. 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.

10.3.8. 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.

10.3.9. 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)

10.3.10. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os serviços.

10.3.11. 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.

10.3.12. 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.

10.3.13. Os serviços serão recebidos definitivamente no prazo de até 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:

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

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

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

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

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

10.3.18. 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.

10.4. **Liquidação:**

10.4.1. Atestado o cumprimento do objeto do contrato pela fiscalização e a correta instrução do processo, após autorização do ordenador, os autos deverão ser remetidos ao setor responsável pela liquidação da despesa e efetivação do pagamento, nos termos do §2º, VII, art. 188, do Decreto Estadual nº 28.874/2024.

10.4.2. 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:

- o prazo de validade;
- a data da emissão;
- os dados do contrato e do órgão contratante;
- o período respectivo de execução do contrato;
- o valor a pagar; e,
- eventual destaque do valor de retenções tributárias cabíveis.

10.4.3. 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;

10.4.4. 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.

10.4.5. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas;

10.4.6. 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.

10.4.7. 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.

10.4.8. 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.

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

10.5. **Prazo de Pagamento**

10.5.1. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de 15 (quinze) dias úteis, conforme dispõe o art. 190, do Decreto Estadual nº 28.874/2024.

10.5.2. 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 ICTI de correção monetária.

10.5.3. Ocorrendo atraso no pagamento em que o Fornecedor não tenha de alguma forma concorrido para a mora, os valores devidos ao Fornecedor serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de correção monetária. Os encargos moratórios pelo atraso no pagamento serão calculados pela seguinte fórmula:

EM = N x Vp x (I / 365)

Onde: EM = Encargos moratórios a serem pagos pelo atraso de pagamento;

N = Números de dias em atraso, contados da data limite fixada para pagamento e a data do efetivo pagamento;

Vp = Valor da parcela em atraso;

I = ICTI anual acumulado (Índice de Custos de Tecnologia da Informação - ICTI do IPEA)/100.

10.6. **Forma de Pagamento**

10.6.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

10.6.4. 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.

10.6.5. 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 (Certificado Digital), de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

10.7. **Cessão de Crédito**

10.7.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020, conforme as regras deste presente tópico.

10.7.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de

2020.

10.7.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos).

10.7.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

11. FORMA E CRITÉRIOS DE SELEÇÃO E REGIME DE EXECUÇÃO (ART. 6º, INCISO XXIII, ALÍNEA 'H', DA LEI N. 14.133/2021).

11.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade pregão, sob a forma eletrônica, com adoção do critério de julgamento **MENOR PREÇO POR GLOBAL**, para os fins de seleção da proposta apta gerar o resultado da contratação mais vantajosa para a Administração Pública, desde que atendidas às especificações constantes deste termo, com fulcro no art. 6º, inciso XLI, da Lei 14.133/21:

11.2. **Exigências de Habilitação**

11.2.1. Previamente à celebração do contrato, a Administração verificará o eventual descumprimento das condições para contratação, especialmente quanto à existência de sanção que a impeça, mediante a consulta a cadastros informativos oficiais, tais como:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

d) Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP emitido pela Controladoria Geral do Estado.

e) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, conforme art. 62, inciso IV, da Lei n. 14.133/2021

11.2.2. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas "b", "c" e "d" acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/).

11.2.3. A consulta aos cadastros será realizada em nome da empresa interessada e de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

11.2.4. Caso conste na Consulta de Situação do interessado a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

11.2.5. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

11.2.6. O interessado será convocado para manifestação previamente a uma eventual negativa de contratação.

11.2.7. Caso atendidas as condições para contratação, a habilitação do interessado será verificada por meio do SICAF, nos documentos por ele abrangidos.

11.2.8. É dever do interessado manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.

11.2.9. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

11.2.10. Se o interessado for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

11.2.11. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11.2.12. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos: que serão exigidos conforme sua natureza jurídica:

11.3. **Habilitação jurídica**

11.3.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.3.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br/;

11.3.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

11.3.4. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

11.3.5. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

11.3.6. No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP- P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, conforme Decreto n° 11.802, de 28/11/2023.

11.3.7. No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 2110, de 2022.

11.3.8. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização, e se for o caso, ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

11.3.9. Os documentos acima deverão estar acompanhados da última alteração ou da consolidação respectiva.

11.4. **Habilitação Fiscal, Social e Trabalhista**

11.4.1. Comprovação de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

11.4.2. Comprovação de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

11.4.3. Prova de regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

11.4.4. Certidão de Regularidade do FGTS, relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

11.4.5. Prova de regularidade perante a Justiça do Trabalho, mediante apresentação de Certidão de Regularidade de Débito – CNDT, para comprovar a

inexistência de débitos inadimplidos perante a Justiça do Trabalho, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento.

11.4.6. **Declaração** de cumprimento do inciso XXXIII do art. 7º da Constituição Federal**.**

11.5. **Qualificação Econômico-Financeira**

11.5.1. Certidão Negativa de feitos sobre falência – Lei n°. 11.101/05, expedida pelo distribuidor da sede do licitante, expedida nos últimos **90 (noventa)** dias caso não conste o prazo de validade - Lei nº 14.133, de 2021, art. 69, *caput*, inciso II);

11.5.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura, caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 5% (cinco por cento) do valor estimado do item/ lote que o licitante estiver participando.

a). No caso do licitante classificado em mais de um item/lote, o aferimento do cumprimento da disposição acima levará em consideração a soma de todos os valores referencias;

b) . Caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns)/lote(s) até o devido enquadramento a regra acima disposta;

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

d) O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

11.5.3. As regras descritas nos incisos "a" e "b", deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

11.5.4. Os documentos referidos acima deverão ser exigidos com base no limite definido nos arts. 1.065 e 1.078 do Código Civil.

11.5.5. Na hipótese de apresentação de Certidão Positiva de recuperação judicial, o (a) Pregoeiro verificará se a licitante teve seu plano de recuperação judicial homologado pelo juízo, conforme determina o art.58 da Lei 11.101/2005.

11.5.6. Eventuais contratos com a Administração Pública e /ou iniciativa privada, vigentes na data da apresentação da proposta, não constituem fato impeditivo para a execução do contrato, objeto deste Termo de Referência.

11.6. A exigência de qualificação econômico-financeira prevista neste Termo de Referência fundamenta-se no art. 69 da Lei Federal nº 14.133/2021 e tem por finalidade assegurar que a futura contratada disponha de capacidade econômico-financeira compatível com o vulto, a complexidade e os riscos associados à execução do objeto.

11.7. Considerando que a contratação possui valor estimado de R$ 33.930.216,36, bem como envolve solução integrada de segurança da informação de elevada criticidade, contemplando o fornecimento de appliances, licenciamento, instalação, configuração, suporte técnico, manutenção, treinamento especializado e solução de segurança avançada, mostra-se pertinente a adoção de requisito adicional de capacidade econômico-financeira, de modo a reduzir o risco de contratação de empresa sem condições financeiras suficientes para suportar os custos decorrentes da implantação e da continuidade da solução.

11.8. A exigência de patrimônio líquido ou capital social mínimo equivalente a 5% (cinco por cento) do valor estimado do item ou lote disputado foi estabelecida em percentual inferior ao limite máximo de 10% (dez por cento) admitido pelo art. 69 da Lei Federal nº 14.133/2021, sendo considerada proporcional ao vulto da contratação e compatível com a necessidade de assegurar capacidade financeira mínima para a execução das obrigações assumidas.

11.9. A pertinência do percentual adotado decorre, ainda, da natureza continuada de parte das obrigações contratuais, especialmente aquelas relacionadas ao suporte técnico, manutenção e à solução de segurança avançada, cuja execução se estenderá pelo período contratual previsto, de modo que eventual incapacidade econômico-financeira da contratada poderá comprometer a continuidade dos serviços de segurança das aplicações e dos ativos tecnológicos da SEDUC-RO.

11.10. O requisito não possui finalidade de restringir a competitividade do certame, mas de estabelecer parâmetro mínimo e proporcional de capacidade financeira, compatível com os riscos decorrentes da contratação, preservando-se, em todo caso, o limite estabelecido no art. 69 da Lei Federal nº 14.133/2021.

11.11. A exigência de patrimônio líquido ou capital social mínimo não se confunde nem se cumula indevidamente com a garantia contratual de execução prevista neste Termo de Referência. Enquanto o requisito de qualificação econômico-financeira constitui condição de habilitação destinada a aferir a capacidade financeira mínima da licitante para assumir o objeto, a garantia contratual possui natureza pós-contratual e finalidade de assegurar o cumprimento das obrigações assumidas pela contratada, constituindo instrumentos de naturezas e finalidades distintas.

11.12. Quanto aos índices econômico-financeiros, serão utilizados exclusivamente indicadores usuais de mercado, destinados à aferição da capacidade de liquidez e solvência da licitante, observados os parâmetros estabelecidos no art. 69 da Lei Federal nº 14.133/2021, devendo sua análise ser realizada de forma objetiva e uniforme para todas as licitantes.Ress

11.13. **Qualificação Técnica**

11.13.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;

11.13.2. 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.

11.14. **Qualificação Técnico-Operacional**

11.14.1. 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.

11.14.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

1) Comprovação de qualificação técnica: A licitante deverá comprovar a execução de serviço de fornecimento de solução de Firewall de Aplicação Web - WAF, proteção das aplicações disponibilizadas na modalidade web, independentemente de sua modalidade, arquitetura ou formato de comercialização (hardware, software ou SaaS).

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

1.2.) Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MP n. 5, de 2017;

2) Deverá haver a comprovação de que a licitante executou serviços satisfatoriamente, por um período mínimo de 6 (seis) meses da execução dos serviços de fornecimento de solução Firewall de Aplicação Web - WAF, com objeto semelhante ao da contratação, podendo ser aceito o somatório de atestados.

11.14.3. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa interessada.

11.14.4. 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 foram prestados os serviços, entre outros documentos.

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

11.14.6. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

11.14.7. A apresentação de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitido, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

11.14.8. Para a presente contratação, serão exigidos a **cópia** dos seguintes documento

11.14.9. Comprovante de Visita Técnica (facultativa) devidamente assinado pelo representante da empresa e pelo representante da SEDUC-RO;

11.14.10. Exame de Conformidade/ Prova Conceito obrigatória em termos de estrutura, aparelhamento e pessoal técnico, às instalações das empresas participantes do certame, detentoras da proposta mais vantajosa, deverão ser submetidas à Exame de Conformidade/Prova Conceito, conforme o Despacho SEDUC/COTIC (0064901234). Esse exame será de responsabilidade de uma equipe técnica da SEDUC-COTIC, a qual emitirá Parecer que poderá, inclusive, ensejar na classificação ou desclassificação da licitante. A solicitação será demanda somente nos casos em que as condições da proposta fornecida não forem suficientes para a corroboração de atendimento das especificações técnicas exigidas; e,

11.14.11. Fornecer catálogos dos produtos, comprovação técnica de todos os itens que compreendem as premissas da solução (através de guias de administração, datasheets, etc.), e planos de instalação com as especificações dos produtos ofertados

11.15. **Da Justificativa da Exigências**

11.16. A exigência de qualificação técnico-operacional estabelecida neste Termo de Referência fundamenta-se no art. 67, §§ 1º e 2º, da Lei Federal nº 14.133/2021, e nas disposições pertinentes do Decreto Estadual nº 28.874/2024, considerando a natureza, a complexidade e os riscos associados à execução da solução integrada de segurança pretendida.

11.17. A contratação compreende solução integrada composta por Firewall de Aplicação Web – WAF, licenciamento, instalação, configuração, manutenção e suporte técnico, treinamento especializado e Solução de Segurança Avançada, destinada à proteção das aplicações institucionais da SEDUC-RO, dos ativos de hardware e software e dos serviços disponibilizados na Internet.

11.18. A exigência de comprovação de experiência anterior na execução de solução de Firewall de Aplicação Web – WAF guarda relação direta com a parcela central e tecnicamente relevante do objeto, tendo em vista que os equipamentos serão implantados em arquitetura de alta disponibilidade e atuarão como ponto central de inspeção, controle e mitigação do tráfego destinado às aplicações institucionais, demandando conhecimento técnico especializado para sua implantação, configuração, operação e manutenção.

11.19. Ressalta-se, ainda, que a Solução de Segurança Avançada constitui componente integrante e tecnicamente relevante da arquitetura contratada, destinada à ampliação da proteção das aplicações expostas à Internet, incluindo mecanismos de proteção contra ataques distribuídos de negação de serviço (DDoS), bots, automações maliciosas, exploração de vulnerabilidades e demais ameaças cibernéticas, além de funcionalidades de avaliação contínua de vulnerabilidades, proteção e gerenciamento de DNS, monitoramento, auditoria e geração de relatórios.

11.20. Considerando que a Solução de Segurança Avançada constitui a parcela de maior valor estimado da contratação, no montante de R$ 12.737.224,28 (doze milhões, setecentos e trinta e sete mil duzentos e vinte e quatro reais e vinte e oito centavos), sua relevância econômica e técnica foi considerada na definição dos requisitos de habilitação. Todavia, a exigência de atestação de capacidade técnico-operacional não será estabelecida de forma desproporcional ou mediante exigência de experiência em marca, fabricante ou solução específica, devendo a comprovação limitar-se à demonstração de experiência anterior compatível com as parcelas relevantes do objeto e suficiente para evidenciar a aptidão operacional da licitante para a execução integral da solução.

11.21. A exigência de experiência anterior em solução WAF, portanto, não se destina a restringir a competitividade do certame, mas a assegurar que a futura contratada possua capacidade operacional compatível com a complexidade e criticidade da solução a ser implantada, considerando a necessidade de integração entre seus componentes, continuidade dos serviços, segurança das aplicações institucionais e mitigação dos riscos decorrentes de falhas de configuração, implantação ou operação.

11.22. Os requisitos estabelecidos observam, assim, os princípios da razoabilidade, proporcionalidade e competitividade, restringindo-se às características indispensáveis à demonstração da aptidão técnica para execução do objeto, vedada a exigência de experiência anterior em tecnologia, fabricante ou modelo específico quando não indispensável à execução contratual.

12. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

12.1. O valor da contratação, é de R$ 33.930.216,36 (trinta e três milhões, novecentos e trinta mil duzentos e dezesseis reais e trinta e seis centavos), conforme o item 9 do Estudo Técnico Preliminar 47 (70175357)

12.2. A estimativa de preços unitários e global que balizará a seleção proposta mais vantajosa, por ocasião do certame licitatório, encontra-se definido conforme o item 9 doEstudo Técnico Preliminar 47 (70175357), em atendimento a competência designativa, cujo montante é da ordem de R$ 33.930.216,36 (trinta e três milhões, novecentos e trinta mil duzentos e dezesseis reais e trinta e seis centavos).

13. DOTAÇÃO ORÇAMENTÁRIA (ART. 92, VII)

13.1. A prestação do serviço, objeto deste estudo, encontra-se previsto no Plano de Contratação Anual - PCA.

13.2. Registra-se, ainda, que a futura contratação será executada com orçamento liberado na Fonte de Recursos 1.500.0.01001, conforme disposto na informação prestada pela Gerência de Execução Orçamentária - SEDUC/GEO - Errata (0060432260).

13.3.

13.4.

13.5.

13.6. Função Progrmática	Natureza de Despesa	Fonte de Recurso
12.122.1015.2398 - Equipar Unidades Educacionais	44.90.52-37 – Equipamentos de TIC - Ativos de Rede	1500001001 - Recursos não vinculados de impostos (Ensino)
12.122.1015.2087- Assegurar a Manutenção Administrativa da Unidade	3.3.90.40.02 - Locação de Software de TIC 3.3.90.40.09 – Serviços Técnicos Profissionais de TIC	1500001001 - Recursos não vinculados de impostos (Ensino)

14. DO JULGAMENTO DA PROPOSTA

14.1. Para julgamento das propostas será adotado o critério de **MENOR PREÇO POR GLOBAL**, observado as especificações técnicas, os parâmetros mínimos de desempenho e de qualidade e as demais condições definidas neste Termo de Referência, estabelecido no ato convocatório designada para a prática do ato.

14.2. A proposta deve ser impressa em papel timbrado da empresa, em uma via, sendo assinada pelo representante legal da empresa, sem emendas, acréscimos, borrões, rasuras, ressalvas, entrelinhas ou omissões, que acarretem lesão ao direito das demais contratadas, prejuízo à administração pública ou impeçam exata compreensão de seu conteúdo, nela deverá conter:

a) Valor unitário mensal;

b) Valor Lote;

14.2.1. Para a prestação dos serviços objeto de contratação, **não foi solicitado** planilha de composição de custos e formação de preços, em virtude de:

a) Não haver mão de obra com dedicação exclusiva, cuja execução não depende da aquisição de insumos específicos para o evento em questão.

14.2.2. Nos preços propostos deverão estar inclusos todas e quaisquer despesas diretas ou indiretas que venham a incidir sobre os mesmos, bem como o custo de materiais, instalação, mão de obra, equipamentos, encargos tributários, trabalhistas e previdenciários, taxas, seguros e outros necessários e indispensáveis à completa execução dos serviços.

14.2.3. Validade da Proposta mínima de 90 (noventa) dias corridos, a partir de seu recebimento pela Administração.

15. DAS OBRIGAÇÕES DA CONTRATANTE (ART. 92, X, XI E XIV)

15.1. Efetuar o recebimento dos serviços verificando se os mesmos estão em conformidade com o Termo de Referência e as cláusulas contratuais.

15.2. Designar, como fiscais do contrato, servidores para executar operacionalmente as ações de acompanhamento físico, controle e fiscalização do contrato, desempenhando o papel de "Representante da Administração" aos termos do art. 177 da Lei nº 14.133/2021.

15.3. Realizar os atos relativos à cobrança do cumprimento pela Contratada das obrigações contratualmente assumidas e aplicar sanções, garantida a ampla defesa e o contraditório, decorrentes do descumprimento das obrigações contratuais.

15.4. Assegurar o acesso dos empregados da Contratada, quando devidamente identificados, aos locais onde irão executar suas atividades.

15.5. Prestar as informações necessárias ao desenvolvimento dos trabalhos.

15.6. Comunicar prontamente à Contratada, qualquer anormalidade no objeto do instrumento contratual, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência.

15.7. Notificar previamente à Contratada, quando da aplicação de sanções administrativas.

15.8. Efetuar o pagamento à Contratada, de acordo com o estabelecido no presente Termo de Referência.

15.9. Fornecer cópia do respectivo Termo de Referência aos responsáveis pela fiscalização e acompanhamento da execução dos serviços para assegurar o controle da qualidade dos serviços prestados, com comprovação de recebimento.

15.10. No início do contrato deve ser realizada inspeção pela contratada, juntamente com a contratante, da quantidade e estado de conservação dos equipamentos que serão postos à disposição da contratada, para que ao terminar o contrato sejam devolvidos em condições de uso.

15.11. Exercer a fiscalização dos serviços realizados pela CONTRATADA, emitindo, mensalmente, relatórios sobre a qualidade dos serviços prestados.

15.12. Exercer a fiscalização de modo a assegurar a execução do serviço contratado, verificando o cumprimento dos horários estabelecidos, utilização de uniformes, de equipamentos e EPIs dentre outros elementos necessários a fiel execução do contrato.

15.13. Solicitar a imediata retirada do local, bem como a substituição de funcionários da CONTRATADA que estiverem sem uniforme ou crachá ou que embaraçarem ou dificultarem a fiscalização do contrato.

15.14. Executar, mensalmente, a medição dos serviços efetivamente prestados, descontando o equivalente aos não realizados, desde que, por motivos imputáveis à CONTRATADA, sem prejuízo das demais sanções disciplinadas no contrato.

15.15. Recusar os materiais e serviços que não estiverem de acordo com as especificações descritas neste Termo de Referência. A ocorrência de não conformidades implicará na não aceitação dos materiais e serviços, devendo a CONTRATADA adotar as medidas necessárias para a sua correção e/ou substituir por produto igual ou similar com anuência da CONTRATANTE, sem ônus para a mesma e sem prejuízo das sanções cabíveis.

15.16. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 20 (vinte) dias.

15.17. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (§4º, do art. 137, da Lei nº 14.133, de 2021).

15.18. 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.

15.19. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

16. DAS OBRIGAÇÕES DA CONTRATADA (ART. 92, XIV, XVI E XVII)

16.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

16.2. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato.

16.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

16.4. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

16.5. Reparar, corrigir, remover, reconstruir ou substituir os serviços, atendimento móvel e reposicionamento de bens, às suas expensas, no total ou em parte, no prazo máximo de 4 (quatro) horas, nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

16.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

16.7. 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 de agente público que tenha desempenhado função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

16.8. Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

16.9. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; 5)certidões que comprovem a regularidade perante a Fazenda Estadual; e, 6) Certidão Negativa de Débitos Trabalhistas – CNDT;

16.10. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante e outras que convier a Administração para o estrito cumprimento de suas obrigações legais;

16.11. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos

trabalhos, bem como aos documentos relativos à execução do empreendimento.

16.12. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

16.13. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

16.14. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

16.15. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

16.16. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

16.17. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para qualificação na contratação direta;

16.18. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

16.19. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

16.20. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

16.21. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

16.22. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

16.23. Garantir o acesso do contratante, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento;

16.24. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o Termo de Referência, no prazo determinado;

16.25. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

16.26. Disponibilizar ao contratante os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

16.27. Autorizar o contratante, no momento da assinatura do contrato, a fazer o desconto nas faturas e realizar os pagamentos dos salários e demais verbas trabalhistas diretamente aos trabalhadores, bem como das contribuições previdenciárias e do FGTS, quando não demonstrado o cumprimento tempestivo e regular dessas obrigações, até o momento da regularização, sem prejuízo das sanções cabíveis;

16.28. Atender às solicitações do contratante quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;

16.29. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo o contratado relatar ao contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

16.30. Instruir seus empregados, no início da execução contratual, quanto à obtenção das informações de seus interesses junto aos órgãos públicos, relativas ao contrato de trabalho e obrigações a ele inerentes, adotando, entre outras, as seguintes medidas:

16.31. Oferecer todos os meios necessários aos seus empregados para a obtenção de extratos de recolhimentos de seus direitos sociais, preferencialmente por meio eletrônico, quando disponível.

16.32. Não se beneficiar da condição de optante pelo Simples Nacional, salvo quando se tratar das exceções previstas no § 5º-C do art. 18 da Lei Complementar nº 123, de 14 de dezembro de 2006;

16.33. Comunicar formalmente à Receita Federal a assinatura do contrato de prestação de serviços mediante cessão de mão de obra, para fins de exclusão obrigatória do Simples Nacional, a contar do mês seguinte ao da contratação, conforme previsão do art.17, XII, art. 30, §1º, II, e do art. 31, II, todos da Lei Complementar nº 123/2006, salvo quando se tratar das exceções previstas no § 5º-C do art. 18 do mesmo diploma legal;

16.34. Para efeito de comprovação da comunicação, a contratado deverá apresentar cópia do ofício enviado à Receita Federal do Brasil, com comprovante de entrega e recebimento, comunicando a assinatura do contrato de prestação de serviços mediante cessão de mão de obra, até o último dia útil do mês subsequente ao da ocorrência da situação de vedação.

16.35. Nos casos em que haja um número mínimo de vinte e cinco colaboradores alocados no contrato, destinar 8% das vagas exclusivamente para mulheres vítimas de violência doméstica;

16.36. As vagas reservadas serão destinadas prioritariamente para pretas e pardas, na proporção que essas mulheres representarem na unidade da federação da prestação do serviço segundo o último censo do IBGE, que no presente caso corresponde a 30%.

16.37. Incluem-se entre as beneficiárias das vagas reservadas as mulheres trans, travestis e outras possibilidades do gênero feminino, conforme definido no art. 5º da Lei nº 11.340, de 7 de agosto de 2006.

16.38. Sempre que houver um desligamento, a contratada deverá buscar atender ao percentual mínimo de 8% com a nova contratação.

16.39. Se não houver mulheres elegíveis em número suficiente para preencher as vagas reservadas, a empresa poderá contratar livremente.

16.40. Para cálculo do percentual de vagas reservadas serão considerados todos os empregados alocados no contrato, incluindo folguistas e substitutos.

16.41. O percentual de mão-de-obra de que trata este item deverá ser mantido durante toda a execução contratual.

16.42. A contratada deve manter o sigilo da condição de violência doméstica da profissional que será alocada para a prestação do serviço.

16.43. Responsabilizar-se integralmente pelos serviços contratados, nos termos da legislação vigente, nos dias e turnos estipulados pela Secretaria Estadual de Educação, bem como na necessidade do serviço em sábados letivos, caso a unidade escolar necessite dos serviços nesses dias, sendo a contratada, comunicada com antecedência de no mínimo 72 horas.

16.44. A Contratada assumirá qualquer responsabilidade pelos encargos judiciais ou extrajudiciais decorrentes da execução dos serviços, que tiver dado causa (s) a terceiro (s).

16.45. Responsabilizar-se pelos danos causados diretamente à administração, aos alunos e terceiros na execução dos serviços, não excluindo ou reduzindo essa responsabilidade pela fiscalização e/ou acompanhamento da Secretaria Estadual de Educação.

16.46. Tratar com urbanidade os alunos, pais, servidores da escola e os agentes de fiscalização da Contratante.

16.47. A Proponente obriga-se ainda, em atendimento ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), a manter sigilo de todas as informações sobre os dados pessoais e dados pessoais sensíveis, repassados em decorrência da execução da contratação, sendo vedado o repasse dessas informações, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do objeto contratado.

16.48. O contratado não compartilhe os recursos humanos e materiais disponíveis de uma contratação para execução simultânea de outros contratos;

16.49. Registrar e controlar, juntamente com a Administração, diariamente, a frequência e a pontualidade de seu pessoal, bem como as ocorrências do posto em que estiver prestando seus serviços.

16.50. A contratada deverá aplicar boas práticas de sustentabilidade em atenção ao art. 170 da CRFB/88, art. 5ª da Lei nº 14.133/202, a Lei nº 12.187/2009 e o art. 6º da Instrução Normativa nº 1/2010 da SLTI/MPOG.

16.51. Deverá ser mantida a disponibilidade de efetivo dentro dos padrões desejados, para atender eventuais acréscimos solicitados pela Administração, bem como impedir que a mão de obra que cometer falta disciplinar, qualificada como de natureza grave, seja mantida ou retorne às instalações dela.

16.52. Comprovar a formação técnica específica da mão de obra oferecida, por meio de Certificado, atestado (s) expedidos por instituições devidamente habilitadas e reconhecidas.

16.53. Apresentar a Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

16.54. Apresentar a Declaração de Fato Superveniente.

16.55. Apresentar a Declaração de ME/EPP.

16.56. Apresentar a Declaração de Ciência do Edital.

16.57. Apresentar a Declaração de Menor.

16.58. Apresentar a Declaração Independente de Proposta.

16.59. Apresentar a Declaração de Acessibilidade.

16.60. Apresentar a Declaração de Cota de Aprendizagem.

16.61. Apresentar a Declaração de Não Utilização de Trabalho Degradante ou Forçado.

17. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

17.1. Comete infração administrativa, nos termos 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.

17.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i)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 nº 14.133, de 2021);

ii) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

17.3. Multa: A aplicação da sanção prevista na alínea “b” observará os seguintes parâmetros:

1) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia útil sobre o valor da parcela em atraso do Contrato, em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia útil e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

2) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor da parcela em atraso do Contrato, em caso de atraso na execução do objeto, por período superior ao previsto no subitem anterior ou de inexecução parcial da obrigação assumida;

3) 0,5% (meio por cento) até 30% (trinta por cento) sobre o valor do Contrato ou do saldo não

atendido do Contrato, em caso de inexecução total da obrigação assumida;

4) 0,2% a 3,2% por dia sobre o valor mensal do Contrato, conforme detalhamento constante das tabelas 1 e 2, abaixo; e

5) 0,07% (sete centésimos por cento) do valor do Contrato por dia útil de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias úteis autorizará o CONTRATANTE a promover a rescisão do Contrato.

6) As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

7) Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo Quadro Abaixo:

INFRAÇÃO			
ITEM	DESCRIÇÃO	GRAU	CORRESPONDÊNCIA
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais, por ocorrência;	05	3,2% ao dia sobre o valor mensal do contrato
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04	1,6% ao dia sobre o valor mensal do contrato
3	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	03	0,8% ao dia sobre o valor mensal do contrato

4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02	0,4% ao dia sobre o valor mensal do contrato
Para os itens a seguir, deixar de:			
5	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02	0,4% ao dia sobre o valor mensal do contrato
6	Substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia;	01	0,2% ao dia sobre o valor mensal do contrato
7	Cumprir quaisquer dos itens do Contrato e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03	0,8% ao dia sobre o valor mensal do contrato
8	Indicar e manter durante a execução do contrato os prepostos previstos no Contrato;	01	0,2% ao dia sobre o valor mensal do contrato

17.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

17.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

17.6. 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, da Lei nº 14.133, de 2021).

17.7. 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, da Lei nº 14.133, de 2021).

17.8. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

17.9. 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.

17.10. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

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.

17.11. 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).

17.12. 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, da Lei nº 14.133, de 2021)

17.13. O Contratante deverá, no prazo máximo de 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, da Lei nº 14.133, de 2021)

17.14. 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.

17.15. 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.

18. GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS (ART. 42, § 1º, II, IV E VII DEC. ESTADUAL Nº 28.874/2024)

18.1. A Superintendência Estadual de Compras e Licitações – SUPEL, será o órgão responsável pelos Atos de Administração, Controle e Gerenciamento da Ata de Registro de Preços, Conforme Decreto Estadual Nº. 28.874, 25 de janeiro de 2024.

18.2. Em atendimento ao disposto no art. 117 e 122, inciso IV, do Decreto nº 28.874/2024, poderá o órgão Gerenciador, caso julgue viável, promover a publicação de Intenção de Registro de Preços – IRP.

19. DA ATA DE REGISTRO DE PREÇOS

19.1. A existência de preços registrados não obriga a Administração a firmar as contratações de que deles poderão advir, facultada a realização de licitação específica para a aquisição pretendida, sendo assegurada à Detentora do registro de preços a preferência em igualdade de condições;

19.2. Fica a Detentora ciente que a publicidade da Ata de Registro de Preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação;

19.3. A Ata de Registro de Preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão ao disposto na Lei n. 14.133/2021, demais normas complementares e disposições da Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos;

19.4. Fica autorizada a utilização da Ata de Registro de Preços pelos órgãos da Administração Direta e Indireta do Estado de Rondônia, em virtude de que o objeto ora licitado é de uso bastante comum, podendo haver interesse por outros órgãos;

19.5. O limite de quantitativo para adesão será gerido pela Superintendência Estadual de Licitações, e não poderá exceder, na totalidade, ao dobro do

quantitativo de cada item registrado, limitado a 50% (cinquenta por cento) para cada órgão não participante que realizar a adesão;

19.6. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras da ata, assumidas com o órgão gerenciador e órgãos participantes;

19.7. Caberá ao órgão que se utilizar da ata, verificar a vantagem econômica da adesão;

19.8. Após publicidade da Ata de Registro de Preços, poderão ser firmados os Contratos dela decorrentes dentro do prazo de validade do Registro, cuja contratação será formalizada pelo Governo do Estado de Rondônia por meio de instrumento contratual, ou ainda, quando for o caso, pela emissão da nota de empenho, ordem de serviço ou outro instrumento similar, conforme dispõe o Art. 95, da Lei n. 14.133/2021;

19.9. A licitante que tenha seus preços registrados obrigar-se-á a cumprir todas as condições dispostas na Ata de Registro de Preços, aplicando-os ao quantitativo solicitado pela Administração;

19.10. O objeto da Ata de Registro de Preços será solicitado de acordo com a necessidade do Governo do Estado de de Rondônia, e a execução será nas condições definidas neste Termo de Referência e na Ata de Registro de Preços.

20. DA ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS E DO CANCELAMENTO

20.1. Art. 132. As eventuais alterações da ata de registro de preços não poderão acarretar aumento dos quantitativos registrados, inclusive, nas hipóteses previstas no art. 124 da Lei Federal n° 14.133, de 2021.

Parágrafo único. Os eventuais contratos decorrentes do registro de preços poderão ser alterados de acordo com as diretrizes da Lei Federal n° 14.133, de 2021, observando-se, quanto aos acréscimos e supressões, a aplicação do limite legal relativo ao contrato individualmente considerado, e não à ata de registro de preços.

20.2. Art. 133. O preço registrado poderá ser revisto em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução tal como pactuado, observada a instrução processual respectiva, cabendo ao órgão gerenciador da ata promover as necessárias negociações junto aos fornecedores.

20.3. Parágrafo único. A alteração dos preços registrados não altera automaticamente os preços dos contratos decorrentes do Sistema de Registro de Preços, cuja revisão deverá ser feita pelo órgão contratante, observadas as disposições legais incidentes sobre os contratos.

20.4. Art. 134. Quando o preço inicialmente registrado, por movo superveniente, tornar-se superior ao preço praticado no mercado o órgão gerenciador deverá convocar o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado.

§ 1° Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados dos compromissos assumidos, sem aplicação de penalidades administravas.

§ 2° A redução do preço registrado será comunicada pelo órgão gerenciador aos órgãos que verem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.

§ 3° A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação obtida originalmente na licitação.

20.5. Art. 135. Quando o preço de mercado se tornar superior aos preços registrados é facultado ao fornecedor requerer, antes do pedido de fornecimento, a atualização do preço registrado, mediante requerimento devidamente instruído com a comprovação de fato superveniente que tenha ensejado a elevação dos preços que inviabilize o cumprimento das obrigações condas na ata, desde que observados os seguintes requisitos.

I - a possibilidade da atualização dos preços registrados seja aventada pelo fornecedor ou prestador signatário da ata de registro de preços;

II - a modificação seja substancial nas condições registradas, de forma que seja caracterizada alteração desproporcional entre os encargos do fornecedor ou prestador signatário da ata de registro de preços e da Administração Pública;

III - seja demonstrado nos autos a desatualização dos preços registrados, por meio de apresentação de planilha de custos e documentação comprobatória correlata que demonstre que os preços registrados se tornaram inviáveis nas condições inicialmente pactuadas.

§ 1° A iniciava e o encargo da demonstração da necessidade de atualização de preço serão do fornecedor ou prestador signatário da ata de registro de preços, cabendo ao órgão gerenciador a análise e deliberação a respeito do pedido.

§ 2° Se não houver prova efetiva da desatualização dos preços registrados e da existência de fato superveniente, o pedido será indeferido pela Administração e o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado na ata, sob pena de cancelamento do registro de preços e de aplicação das penalidades administravas previstas em lei e no edital.

§ 3° Na hipótese do cancelamento do registro de preços prevista no § 2° deste artigo, o órgão gerenciador poderá convocar os demais fornecedores integrantes do cadastro de reserva para que manifestem interesse em assumir o fornecimento dos bens, a execução das obras ou dos serviços, pelo preço registrado na ata.

§ 4° Comprovada a desatualização dos preços registrados decorrente de fato superveniente que prejudique o cumprimento da ata, a Administração poderá efetuar a atualização do preço registrado, adequando-o aos valores praticados no mercado.

§ 5° Como alternava à atualização prevista no parágrafo anterior, o órgão gerenciador poderá liberar o fornecedor do compromisso assumido, sem aplicação de qualquer penalidade.

§ 6° Liberado o fornecedor na forma do parágrafo anterior, o órgão gerenciador poderá convocar os integrantes do cadastro de reserva, para que manifestem interesse em assumir o fornecimento dos bens, a execução das obras ou dos serviços, pelo preço registrado.

§ 7° Na hipótese de não haver cadastro de reserva, a Administração Pública poderá convocar os licitantes remanescentes, na ordem de classificação, para negociação e assinatura da ata no máximo nas condições ofertadas por estes, desde que o valor seja igual ou inferior ao orçamento esmado para a contratação, inclusive quanto aos preços atualizados, nos termos do instrumento convocatório.

§ 8° Não havendo êxito nas negociações, o órgão gerenciador deverá proceder ao cancelamento da ata de registro de preços, adotando de imediato as medidas cabíveis para a satisfação da necessidade administrava.

21. DA JUSTIFICATIVA PARA ADOÇÃO DO SISTEMA DE REGISTRO DE PREÇOS:

21.1. Sabe-se que o registro de preço é uma das modalidades de escolha para as aquisições públicas pelas características que se impõem através do Art. 40 da Lei 14.133/21.

21.2. O registro de preços é um sistema que visa uma racionalização nos processos de contratação de compras públicas e de prestação de serviços. Sua finalidade precípua é maximizar o princípio da economicidade, permitindo à Administração Pública celebrar o contrato administrativo na exata medida e no momento de sua necessidade, sempre precedido de licitação, qualquer que seja o valor efetivo a ser praticado em cada situação específica.

21.3. No registro de preços não há quantidade mínima a ser adquirida, tampouco obrigatoriedade de aquisição de todo o quantitativo licitado. Os valores registrados não são exclusivos para determinadas secretarias ou entidades e podem ser compartilhados por toda a administração, dentro dos limites esculpidos pela legislação.

21.4. **Da fundamentação técnica para adoção do Sistema de Registro de Preços:**

21.4.1. A manutenção da adoção do Sistema de Registro de Preços permanece tecnicamente justificada e compatível com as características da contratação, enquadrando-se nas hipóteses previstas no **art. 116 do Decreto Estadual nº 28.874/2024**, especialmente pelos incisos aplicáveis à presente contratação, considerando que:

a) **a demanda possui execução parcelada e sucessiva**, uma vez que a implantação da solução ocorrerá em etapas distintas, observando cronograma técnico previamente estabelecido, sem que haja conveniência ou viabilidade operacional para o fornecimento e implantação integral em um único momento;

b) **não é possível definir, com precisão absoluta, o momento de consumo integral dos quantitativos registrados** , pois a evolução das etapas dependerá da conclusão das atividades de implantação, migração, homologação, estabilização operacional e validação técnica da infraestrutura instalada, circunstâncias inerentes a projetos de infraestrutura crítica de Tecnologia da Informação;

c) **a contratação envolve solução tecnológica cuja implantação demanda acompanhamento contínuo, operação assistida e validação progressiva**, sendo necessária a realização de testes de desempenho, disponibilidade, interoperabilidade, segurança, contingência e recuperação de desastres antes da expansão da solução para os demais ambientes computacionais.

21.5. No presente caso, a solução contempla equipamentos destinados à proteção das aplicações corporativas críticas da SEDUC/RO, responsáveis pelo atendimento dos sistemas institucionais utilizados por estudantes, servidores, unidades escolares e demais usuários dos serviços digitais da Secretaria.

21.6. Em razão da elevada criticidade do ambiente tecnológico, a implantação será realizada de forma gradativa, iniciando pelo **Datacenter Principal (PRM – Datacenter A)**, onde serão executadas todas as atividades de instalação, configuração, migração das políticas de segurança, integração com a infraestrutura existente, testes de carga, validação funcional, ajustes operacionais e operação assistida.

21.7. Somente após a conclusão dessas etapas, comprovação da estabilidade operacional da solução e emissão do respectivo aceite técnico será iniciada a implantação da infraestrutura destinada ao **Datacenter de Recuperação de Desastres (DR – Datacenter B)**.

21.8. Essa estratégia reduz significativamente os riscos de indisponibilidade dos sistemas corporativos, evita impactos na prestação dos serviços públicos, assegura maior confiabilidade ao ambiente computacional e permite que eventuais ajustes sejam realizados antes da expansão da solução para o ambiente de contingência.

21.9. Além dos aspectos técnicos, a adoção do Sistema de Registro de Preços possibilita que o consumo dos quantitativos registrados ocorra de forma gradual, conforme a efetiva evolução da implantação, evitando aquisições antecipadas desnecessárias, preservando a eficiência da gestão contratual, a racionalização da execução orçamentária e o adequado gerenciamento do saldo da Ata de Registro de Preços.

21.10. Os quantitativos registrados foram definidos mediante critérios técnicos constantes da Memória de Cálculo do Estudo Técnico Preliminar, considerando o levantamento da infraestrutura existente, capacidade de processamento necessária, requisitos de alta disponibilidade, crescimento projetado da demanda, histórico da contratação anterior, necessidade de atualização tecnológica e critérios de segurança cibernética.

21.11. Dessa forma, embora o quantitativo esteja previamente dimensionado, sua execução ocorrerá de forma sucessiva e planejada, situação plenamente compatível com o Sistema de Registro de Preços e com as hipóteses autorizadoras previstas no art. 116 do Decreto Estadual nº 28.874/2024, garantindo aderência aos princípios da eficiência, planejamento, economicidade, continuidade dos serviços públicos e gestão de riscos.

21.12. Importa destacar que a opção pelo Sistema de Registro de Preços não decorre de incerteza quanto ao quantitativo total da solução, o qual se encontra integralmente definido na Memória de Cálculo do Estudo Técnico Preliminar, mas sim da necessidade de que a execução física e financeira da contratação ocorra de forma escalonada, acompanhando a evolução da implantação, a validação técnica de cada ambiente e a mitigação dos riscos inerentes à substituição de infraestrutura crítica de segurança da informação. Assim, o SRP constitui instrumento de gestão contratual compatível com a natureza do objeto, permitindo o consumo planejado dos quantitativos registrados ao longo da vigência da Ata, em conformidade com o planejamento institucional e com os princípios da eficiência, economicidade e continuidade dos serviços públicos.

21.13. Levando em conta as prerrogativas acima descritas JUSTIFICA-SE a necessidade do registro de preços para pretensa aquisição constante neste termo de referência conforme discriminação e quantitativos estabelecidos.

21.14. O órgão gerenciador da Ata de Registro de Preço será a Coordenadoria do Sistema de Registro de Preço-CRP/SUPEL/RO.

21.15. A Secretaria de Estado da Educação é o único órgão participante da Ata de Registro de Preços.

22. DA UTILIZAÇÃO DA ATA E DO FORNECIMENTO ADICIONAL "CARONAS"

22.1. Esta Ata de Registro de Preços poderá ser utilizada por qualquer órgão da Administração Direta e Indireta, inclusive autarquias e fundações do GOVERNO DE RONDÔNIA, ou qualquer outro Órgão tanta da Esfera Estadual, quanto Municipal, mediante consulta ao órgão gerenciador nos termos da Lei vigente.

22.2. A utilização de ata de registro de preço por órgão não participante está sujeita à prévia autorização do órgão gerenciador, nos termos do art 124, § 5º, do Decreto Estadual 28.874, de 25 de janeiro de 2024;

§ 5°. As solicitações de adesão deverão ser formalizadas por meio de requerimento específico instruído em processo administrativo próprio com os seguintes documentos:

I - documento que ateste a equivalência do objeto registrado com a necessidade administrativa do órgão não participante;

II - nota de reserva orçamentária do recurso necessário a fazer face à despesa decorrente da adesão;

III - demonstração da vantajosidade dos preços registrados por meio da realização de pesquisa de mercado com amplitude e diversidade de fontes;

IV - autorização expressa do órgão gerenciador;

V - autorização expressa do fornecedor ou prestador de serviço registrado nos moldes previstos no § 4° deste artigo.

22.3. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão a ata de registro de preços da Administração Pública Estadual;

22.4. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente da adesão, desde que não prejudique as obrigações presentes e futuras da ata, assumidas com o órgão gerenciador e órgãos participantes;

22.5. Conforme disposto no art. 121 do decreto estadual 28.874/2024, o limite individual da cada órgão ou entidade não participante será de um aumento de 50% do quantitativo registrado, ressalvado o disposto no ressalvado o disposto no art. 86, § 7°, da Lei Federal n° 14.133, de 2021.

22.6. As adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o Órgão gerenciador e aos Órgãos participantes, independentemente do número de Órgãos não participantes que aderirem;

22.7. A quantidade mínima para cada ordem de fornecimento, será de 10% (dez por cento), do quantitativo registrado, conforme art. 121 do Decreto Estadual n° 28.874/24.

22.8. Caberá ao órgão que se utilizar da ata, verificar a vantagem econômica da adesão a este Registro de preços.

22.9. Caso haja adesão de itens individualizados, estes devem corresponder à proposta de menor valor, sob pena de inviabilidade da adesão.

22.10. A utilização da ata de registro de preço por órgão não participante está sujeita a prévia autorização do órgão gerenciador.

23. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

23.1. O registro de preço de fornecedor ou prestador de serviço será cancelado quando:

23.1.1. For atestado o descumprimento das condições previstas na ata de registro de preços;

23.1.2. O contrato ou documento equivalente não for firmado no prazo estabelecido pela Administração;

23.1.3. O fornecedor ou prestador de serviço registrado não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aos preços praticados no

mercado;

23.1.4. Estiverem presentes razões de interesse público; e

23.1.5. Restar caracterizada a impossibilidade de concretização do objeto registrado em razão de caso fortuito ou força maior.

23.2. O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do órgão gerenciador, após manifestação da fiscalização contratual.

23.3. O disposto no § 1° do art. 136 do Decreto 28.874/2024 poderá ser observado nas hipóteses de cancelamento do registro, sem prejuízo da prévia negociação para obtenção de condições mais vantajosas para a Administração.

24. DAS OBRIGAÇÕES DO GERENCIADOR E DA DETENTORA

24.1. DO GERENCIADOR

24.1.1. Compete ao Gerenciador, dentre outras atividades estabelecidas na ata de registro de preços:

a) A condução do conjunto de procedimentos para o registro de preços e gerenciamento da ata de registro de preços dela decorrente.

b) Informar aos demais órgãos da administração pública sobre a sua intenção de registrar preços dos itens previamente definidos.

c) A prática de todos os atos de controle e administração do Sistema de Registro de Preços.

24.2. DA DETENTORA

24.2.1. Além de outras obrigações definidas na Ata de Registro de Preços, a detentora da Ata deverá:

a) Estar devidamente licenciada junto aos órgãos de fiscalização do objeto licitado, podendo ser fiscalizada, a qualquer tempo, pelo Órgão Gerenciador.

b) Efetuar a entrega dos produtos nas quantidades, prazos e locais estabelecidos no Instrumento Convocatório.

25. DA APLICAÇÃO DA COTA RESERVADA

25.1. Afastamos a possibilidade de reserva da cota prevista no Inciso XII Art. 42 do Decreto 28.874/2024, de 25 de janeiro de 2024, para os beneficiários da Lei Complementar Federal nº 123, de 2006, tendo em vista o seguinte:

25.2. A aplicação da Cota Reserva relativo ao tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte, quando se trata SERVIÇOS, não pode ser adotada por falta de amparo legal , com fulcro no inciso III, art. 48 da Lei Complementar nº 123/2026, art. 48, inciso III, hipótese prevista XII, art. 42, do Decreto Estadual nº 28.874/2024.

26. DA INTENÇÃO DE REGISTRO DE PREÇOS (IRP)

26.1. Em conformidade com o disposto nos artigos 117 e 122, inciso IV, do Decreto nº 28.874/2024, o órgão Gerenciador não poderá promover a publicação da **Intenção de Registro de Preços (IRP)**, uma vez que o objeto em questão é de natureza específica da **Secretaria de Estado da Educação (SEDUC)**. A ampla divulgação poderá comprometer o andamento do processo. Além disso, o procedimento está alinhado ao desenvolvimento das atividades laborais diárias de diverso setores da estrutura da SEDUC, que devem conciliar suas atividades rigorosamente em função do calendário escolar em todo o Estado de Rondônia. Assim, a não publicação da IRP visa resguardar a integridade e a regularidade do processo licitatório, conforme a legislação vigente.

27. FORMAÇÃO DO CADASTRO DE RESERVAS

27.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro, dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e dos licitantes que mantiverem sua proposta original

28. DA RESOLUÇÃO DE CONFLITOS

28.1. Nesta contratação serão empregados meios alternativos para a resolução pacífica de conflitos, desde que as controvérsias não estejam relacionadas com direitos patrimoniais indisponíveis, considerando o Princípio da Indisponibilidade, na forma da Constituição Federal e do Capítulo XII da Lei Federal 14.133/21.

28.2. Caso não seja possível a resolução pacifica, fica eleito o foro do Município de Porto Velho/RO, em renúncia a qualquer outro, por mais privilegiado que seja.

29. DA EXTINÇÃO CONTRATUAL (ART. 92, XIX)

29.1. Em caso de descumprimento de quaisquer das condições estabelecidas neste instrumento, a extinção do contrato, seja administrativa ou amigável, será efetuada de acordo com as disposições do art. 137 e seguintes da Lei nº 14.133/2021 e demais ordenamentos jurídicos, conforme estipulado nos itens 11.1 a 11.11.2. do Termo de Contrato.

30. CONSIDERAÇÕES FINAIS

30.1. A publicação dos atos deverá se dar no Diário Oficial do Estado e demais meios usualmente adotados.

31. ANEXOS

ANEXO I- Minuta de Contrato

ANEXO II - SAMS

Documento assinado eletronicamente por **Fabiano do Nascimento Lima**, **Coordenador(a)**, em 07/08/2026, às 14:34, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Massud Jorge Badra Neto**, **Secretário(a)**, em 07/08/2026, às 15:50, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.