TERMO DE REFERÊNCIA

Número do Processo - SISLOG
107439
Número do Processo - SEI
202400005025454

Em conformidade com a Lei federal nº 14.133, de 01 de abril de 2021 e com o Decreto estadual n° 10.207, de 27 de janeiro de 2023, o Termo de Referência é o documento necessário para a contratação de bens e serviços comuns, destinado a identificar as especificações do objeto e as condições da contratação e execução, devendo conter os elementos mínimos previstos na legislação.

O Termo de Referência deve ser elaborado com base nos estudos técnicos preliminares, após o posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina.

O Termo de Referência deverá ser elaborado, obrigatoriamente, nas contratações de bens e serviços comuns, inclusive serviços comuns de engenharia, independente da forma de seleção do fornecedor, seja por licitação ou por contratação direta.

Tópico 1 - DADOS DA CONTRATAÇÃO

1.1. Dados do Processo	Número do Processo Administrativo no Sei 202400005025454
1.2. Adequação Orçamentária	A presente contratação será autorizada pelo Ordenador de Despesas, com a respectiva indicação orçamentária, nos termos do Decreto estadual n° 10.207, de 27 de janeiro de 2023.

Tópico 2 - DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO

2.1. Descrição resumida do objeto	Fornecimento de Bens e Materiais e Serviços - Expansão de Solução de Application Delivery Controller (ADC)
2.2. Regime de fornecimento de bens ou serviços	Fornecimento de Bens e Materiais e Serviços por empreitada por preço unitário, nos termos do Cronograma constante neste TR (se aplicável).
2.3. Natureza da execução do objeto	Fornecimento de Bens e Materiais e Serviços: Continuada
2.4. Característica do objeto	Comum, conforme justificativa constante do Estudo Técnico Preliminar.
2.5. Instrumento Contratual	A presente contratação será formalizada por meio de Termo de Contrato.
2.6. Prazo de vigência contratual	O prazo de vigência contratual é de 60 meses, contados imediatamente após a divulgação no Portal Nacional de Contratações Públicas (PNCP), nos termos do Título III, Capítulo V, daLei federal nº 14.133, de 01 de abril de 2021. Considerando que o objeto contratado é de natureza [naturezaObjeto], a vigência do contrato é prorrogável nos termos do art. 106 da Lei federal nº 14.133, de 01 de abril de 2021. A minuta de Termo de Contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

Tópico 3 - ESTIMATIVAS DO VALOR DA CONTRATAÇÃO E DOS PREÇOS REFERENCIAIS

3.1. Os valores referenciais estimados da contratação, unitários e totais, aferidos conforme ampla pesquisa de mercado, são os seguintes:

Item	Descrição	Quantidade	Valor Unit	Valor Total
1	Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R10900	2	R$ 861.720,00	**R$ 1.723.440,00**
2	Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R10900	2	R$ 2.952.680,00	**R$ 5.905.360,00**
3	Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R5900	2	R$ 531.060,00	**R$ 1.062.120,00**
4	Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R5900	2	R$ 1.897.400,00	**R$ 3.794.800,00**
5	F5 TAP Standard Services (pacote com 4 horas, horário comercial)	15	R$ 13.500,00	**R$ 202.500,00**
6	F5 TAP Premium Services (pacote com 4 horas, fora do horário comercial)	2	R$ 40.000,00	**R$ 80.000,00**
7	Treinamento oficial F5 LTM Instructor-led (por aluno)	4	R$ 9.000,00	**R$ 36.000,00**
8	Treinamento oficial F5 ASM Instructor-led (por aluno)	4	R$ 17.000,00	**R$ 68.000,00**
		VALOR TOTAL		**R$ 12.872.220,00**

3.1.1. Abaixo detalhamento dos itens:

Lote Único	
Descrição do item 001 Código 6384 - Controlador de Entrega de Aplicações (Application Delivery Controller - ADC), 256 GB, 20 portas, 10 GbE, 25 GbE.	
Informações Adicionais Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R10900	
Quantidade	2
Unidade	unidade
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo

Valor Unitário	R$ 861.720,00
Valor Total	R$ 1.723.440,00

Lote Único	
Descrição do item 002 Código 5262 - Subscrição de Uso de Software, Subscrição com atualização do software, garantia e suporte técnico.	
Informações Adicionais Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R10900	
Quantidade	2
Unidade	unidade
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 2.952.680,00
Valor Total	R$ 5.905.360,00

Lote Único	
Descrição do item 003 Código 6384 - Controlador de Entrega de Aplicações (Application Delivery Controller - ADC), 256 GB, 20 portas, 10 GbE, 25 GbE.	
Informações Adicionais Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R5900	
Quantidade	2
Unidade	unidade
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 531.060,00
Valor Total	R$ 1.062.120,00

Lote Único	
Descrição do item 004 Código 5262 - Subscrição de Uso de Software, Subscrição com atualização do software, garantia e suporte técnico.	
Informações Adicionais Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R5900	
Quantidade	2
Unidade	unidade
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 1.897.400,00
Valor Total	R$ 3.794.800,00

Lote Único	
Descrição do item 005 Código 5989 - Suporte Técnico, remoto, para software.	
Informações Adicionais F5 TAP Standard Services (pacote com 4 horas, horário comercial)	
Quantidade	15
Unidade	servico (s)
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 13.500,00
Valor Total	R$ 202.500,00

Lote Único	
Descrição do item 006 Código 5989 - Suporte Técnico, remoto, para software.	
Informações Adicionais F5 TAP Premium Services (pacote com 4 horas, fora do horário comercial)	
Quantidade	2
Unidade	servico (s)
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 40.000,00
Valor Total	R$ 80.000,00

Lote Único	
Descrição do item 007 Código 909 - Capacitação Profissional, treinamento técnico de equipe.	
Informações Adicionais Treinamento oficial F5 LTM Instructor-led (por aluno)	
Quantidade	4
Unidade	servico (s)
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 9.000,00
Valor Total	R$ 36.000,00

Lote Único	
Descrição do item 008 Código 909 - Capacitação Profissional, treinamento técnico de equipe.	
Informações Adicionais Treinamento oficial F5 ASM Instructor-led (por aluno)	
Quantidade	4
Unidade	servico (s)
Participação	Ampla Participação
Local de Entrega	secretaria-geral de governo
Valor Unitário	R$ 17.000,00
Valor Total	R$ 68.000,00

3.2. Preço Total Estimado: não sigiloso - **R$ 12.872.220,00 (Doze milhões, oitocentos e setenta e dois mil, duzentose vinte reais)** .

3.3. O preço total estimado da contratação fundamenta-se conforme pesquisa de preços realizada em conformidade com o Decreto estadual n° 9.900, de 07 de julho de 2021.

3.4. Os preços estimados especificados neste Termo de Referência, unitários, totais e global, correspondem aos preços máximos nos quais o objeto poderá ser adjudicado. Não será admitida a adjudicação do objeto por preços (unitário e global) superiores aos especificados neste Termo de Referência.

Tópico 4 - DESCRIÇÃO DETALHADA DO OBJETO

4.1. O objeto contratado deverá atender às especificações e a descrição como um todo, abaixo apresentadas:

4.1.1. A Expansão de Solução de Application Delivery Controller (ADC) consiste dos seguintes equipamentos, licenciamento e serviços:

Item	Descrição	Quantidade
1	Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R10900	2
2	Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R10900	2
3	Equipamento - Appliance ADC (Application Delivery Controller) BIG IP R5900	2
4	Subscrição com upgrade de software (Best Bundle, IPi,Threat Campaigns), Garantia e Suporte Técnico (60 meses) para Appliance ADC BIG IP R5900	2
5	F5 TAP Standard Services (pacote com 4 horas, horário comercial)	15
6	F5 TAP Premium Services (pacote com 4 horas, fora do horário comercial)	2
7	Treinamento oficial F5 LTM Instructor-led (por aluno)	4
8	Treinamento oficial F5 ASM Instructor-led (por aluno)	4

4.2. Requisitos Gerais de Hardware Comum aos Itens 1 e 3 (Appliances Físicos):

4.2.1. 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;

4.2.2. Todos os equipamentos fornecidos e seus componentes deverão ser novos, sem utilização anterior, em linha de fabricação na data da entrega e com previsão de suporte do fabricante durante toda a vigência do contrato;

4.2.3. Os equipamentos deverão ser entregues e instalados nos Data Centers Corporativos do Governo do Estado de Goiás (DC1 e DC2) localizados nos endereços listados no item 7.1.2.

4.2.4. Na data da proposta, nenhum dos modelos dos equipamentos pode estar listado no site do fabricante como EoS (End of Sale) ou EoL (End of Life/Support), durante o período do contrato;

4.2.5. Caso o modelo dos equipamentos ofertados já tenha sido anunciado pelo fabricante, até a data da assinatura do contrato, como EoS (End of Sale) ou EoL (End of Life/Support), deverão ser fornecidos equipamentos da linha que venham a suceder a anterior, com características iguais ou superiores ao modelo ofertado;

4.2.6. As subscrições de garantia e suporte do fabricante de todos os equipamentos e softwares envolvidos na solução serão de responsabilidade da CONTRATADA, que deverá mantê-las ativas durante toda a vigência do contrato;

4.2.7. Qualquer componente de hardware e software da solução deverá ser entregue e mantido com todas as licenças necessárias para seu pleno funcionamento de acordo com esse Termo de Referência, durante toda a vigência do contrato;

4.2.8. 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;

4.2.9. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

4.2.10. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário;

4.2.11. Possuir fontes de alimentação redundantes AC bivolt internas, com ajuste automático de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz), capaz de sustentar a carga de todo o equipamento com todas as portas ativas com apenas umas das fontes instalada e permitir a troca da fonte redundante com o equipamento em pleno funcionamento;

4.2.12. Deverão ser fornecidos os cabos de alimentação para as fontes com conectores C13/C15 e C14;

4.2.13. Permitir operação normal em temperaturas de 0ºC até 40ºC e umidade relativa de 5% a 85% (sem condensação);

4.2.14. Possuir, no mínimo, as características de conectividade:

4.2.14.1. Possuir, no mínimo, 1 porta de gerenciamento Ethernet 1000BASE-T out-of-band;

4.2.14.2. Possuir, no mínimo, 1 porta USB 3.0;

4.2.14.3. Possuir, no mínimo, 1 porta de console serial;

4.2.14.4. Suportar agregação de portas baseado no protocolo LACP, em modo passivo e ativo, com pelo menos 8 portas em um mesmo conjunto agregado;

4.2.14.5. Suportar a Spanning-Tree (802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s);

4.2.14.6. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;

4.2.14.7. Permitir configurar, pelo menos, 2.000 (duas mil) VLANs;

4.3. Características específicas Item 1 (Equipamento - Appliance ADC BIG IP R10900):

4.3.1. Possuir, no mínimo, 16 (dezesseis) portas 10/25 Gigabit Ethernet SFP+/SFP28, acompanhado de 4 (quatro) transceivers 25GBase-SR para fibras multimodo com conectores do tipo LC (por appliance);

4.3.2. Possuir, no mínimo, 4 (quatro) portas 40/100 Gigabit Ethernet QSFP+/QSFP28, devendo ser acompanhado de 4 (quatro) cabos AOC (ActiveOptical Cables) QSFP28/QSFP28 de 100Gbps e 30 (trinta) metros de comprimento (por appliance);

4.3.3. Possuir, no mínimo, 2 discos SSD configurados em RAID-1;

4.3.4. Deve suportar, no mínimo, as seguintes características de desempenho:

4.3.5. 190 (cento e noventa) Gbps em camada 4 do modelo OSI;

4.3.6. 190 (cento e noventa) Gbps em camada 7 do modelo OSI;

4.3.7. 2,5 (dois vírgula cinco) milhões de conexões por segundo na camada 4 do modelo OSI;

4.3.8. 180 (cento e oitenta) milhões de conexões simultâneas na camada 4 do modelo OSI;

4.3.9. 6,6 (seis vírgula seis) milhões de requisições por segundo na camada 7 do modelo OSI;

4.3.10. 95 (noventa e cinco) Gbps de throughput para tráfego SSL/TLS;

4.3.11. 140.000 (cento e quarenta) mil transações SSL por segundo, considerando cifras ECDHE-ECDSA P-256;

4.3.12. 110.000 (cento e dez) mil transações SSL por segundo, considerando cifras ECDHE P-256-RSA 2k;

4.3.13. 200.000 (duzentas) mil transações SSL por segundo, considerando o uso de RSA com chaves de 2.048 (dois mil e quarenta e oito) bits;

4.3.14. 90 (noventa) Gbps de compressão em hardware;

4.3.16. 160 (cento e sessenta) milhões SYN Cookies/segundo;

4.3.17. Suportar, no mínimo, 36 (trinta e seis) instâncias virtuais isoladas entre si, com sistema operacional, plano e controle e plano de dados próprios, inclusive de versões diferentes, e reserva de recursos.

4.4. Características específicas Item 3 (Equipamento - Appliance ADC BIG IP R5900):

4.4.1. Possuir, no mínimo, 8 (oito) portas 10/25 Gigabit Ethernet SFP+/SFP28, acompanhado de 4 (quatro) transceivers 25GBase-SR para fibras multimodo com conectores do tipo LC (por appliance);

4.4.2. Possuir, no mínimo, 2 (duas) portas 40/100 Gigabit Ethernet QSFP+/QSFP28, devendo ser acompanhado de 2 (dois) cabos AOC (Active Optical Cables) QSFP28/QSFP28 de 100Gbps e 30 (trinta) metros de comprimento (por appliance);

4.4.3. Possuir, no mínimo, 1 disco SSD;

4.4.4. Deve suportar, no mínimo, as seguintes características de desempenho:

4.4.5. 95 (noventa e cinco) Gbps em camada 4 do modelo OSI;

4.4.7. 95 (noventa e cinco) Gbps em camada 7 do modelo OSI;

4.4.8. 1,8 (um vírgula oito) milhões de conexões por segundo na camada 4 do modelo OSI;

4.4.9. 100 (cem) milhões de conexões simultâneas na camada 4 do modelo OSI;

4.4.10. 4,3 (quatro vírgula três) milhões de requisições por segundo na camada 7 do modelo OSI;

4.4.11. 50 (cinquenta) Gbps de throughput para tráfego SSL/TLS;

4.4.12. 70.000 (setenta) mil transações SSL por segundo, considerando cifras ECDHE-ECDSA P-256;

4.4.13. 55.000 (cinquenta e cinco) mil transações SSL por segundo, considerando cifras ECDHE P-256-RSA 2k;

4.4.14. 100.000 (cem) mil transações SSL por segundo, considerando o uso de RSA com chaves de 2.048 (dois mil e quarenta e oito) bits;

4.4.15. 50 (cinquenta) Gbps de compressão em hardware;

4.4.16. 80 (oitenta) milhões SYN Cookies/segundo;

4.4.17. Suportar, no mínimo, 26 (vinte e seis) instâncias virtuais isoladas entre si, com sistema operacional, plano e controle e plano de dados próprios, inclusive de

versões diferentes, e reserva de recursos.

4.5. Requisitos Gerais de Software Comuns aos Itens 2 e 4 (Subscrições):

4.5.1 Devem ser entregues subscrições de garantia e suporte do fabricante, na modalidade Premium Support, por 60 meses, incluindo os pacotes Best Bundle, IP Inteligence (IPI) e Threat Campaigns;

4.5.2. Os serviços de suporte técnico e garantia deverão ser prestados pela CONTRATADA e pelo fabricante nas formas on-site ou remoto e no regime 24X7;

4.5.3. Deverá garantir o acesso às atualizações pelo período de abrangência do contrato;

4.5.4. As subscrições deverão ser do fabricante e disponibilizadas para vinculação na conta/perfil da CONTRATANTE no portal de suporte do fabricante.

4.5.5. Suportar IPv4 e IPv6;

4.5.6. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;4.5.7 Suportar VXLAN para integração com ambiente de virtualização;

4.5.8. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;

4.5.9. Suportar implementação em alta disponibilidade com os seguintes requisitos:

4.5.9.1. Implementar modo ativo/standby, com equipamento da mesma marca e modelo;

4.5.9.2. Suportar modo ativo/ativo para, pelo menos, as funções de ADC. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

4.5.9.3. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;

4.5.9.4. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, heartbeat e sincronização entre os equipamentos;

4.5.9.5. Suportar todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

4.5.9.6. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;

4.5.1.0 Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento, com os seguintes requisitos:

4.5.10.1. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

4.5.10.2. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;

4.5.10.3. Manter internamente múltiplos arquivos de configurações do sistema;

4.5.10.4. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;

4.5.10.5. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;

4.5.10.6. Permitir a configuração de múltiplas contas locais de administradores;

4.5.10.7. 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;

4.5.10.8. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;

4.5.10.9. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;

4.5.10.10. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;

4.5.10.11. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;

4.5.10.12. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

4.5.10.13. Suportar a rollback de configuração e imagem;

4.5.10.14. 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;

4.5.10.15. Implementar limitação da taxa (rate limit) de 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;

4.5.10.16. Permitir reiniciar o equipamento pela interface gráfica e por CLI;

4.5.10.17. Implementar SNMPv1, SNMPv2c e SNMPv3;

4.5.10.18. Suportar o envio de traps SNMP, a um ou mais servidores de monitoramento configurados;

4.5.11. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos com as seguintes características:

4.5.11.1. Coleta de métricas de desempenho compatível com Prometheus;

4.5.11.2. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;

4.5.11.3. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, DataDog, ElasticSearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka, OpenTelemetry, Splunk e StatsD;

4.5.11.4. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;

4.5.11.5. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;

4.5.11.6. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e membros do pool;

4.5.11.7. Deve incluir métricas de throughtput, conexões, bits, pacotes, disponibilidade;

4.5.11.8. Deve incluir métricas de requisições e respostas;

4.5.11.9. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;

4.5.11.10. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;

4.5.11.11. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;

4.5.11.12. 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;

4.5.11.13. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);

4.5.11.14. Deve incluir métricas do cluster, incluindo data de sincronização;

4.5.11.15. Deve incluir informações de data da última configuração aplicada;

4.5.11.16 Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;

4.5.12. Implementar debugging utilizando CLI via console e SSH;

4.5.13. Possuir ferramenta interna de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;

4.5.14. 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;

4.5.15. 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;

4.5.16. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;

4.5.17. 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;

4.5.18. 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;

4.5.19. Implementar roteamento IPv4 e IPv6 estático e dinâmico, e todas as seguintes características devem ser suportadas em ambos os protocolos;

4.5.19.1. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas;

4.5.19.2. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP;

4.5.19.3. Suportar integração via BGP para divulgação de prefixos;

4.5.19.4. 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;

4.5.19.5. Deve suportar Equal Cost Multipath (ECMP);

4.5.19.6. Implementar Bidirectional Forward Detection (BFD);

4.5.20. Requisitos da funcionalidade de entrega de aplicações (ADC);

4.5.20.1. Implementar funções de entrega de aplicações através do balanceamento de servidores com qualquer hardware, sistema operacional e tipo de aplicação;

4.5.20.2. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3;

4.5.20.3. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;

4.5.20.4. 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;

4.5.20.5. Implementar criptografia de cookies;

4.5.20.6. 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 ou origem, por sessão SSL, parâmetros da URL acessada, parâmetro no cabeçalho HTTP, ou qualquer informação do payload de camada 7;

4.5.20.7. 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;

4.5.20.8. 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;

4.5.20.9. 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;

4.5.20.10. Suportar balanceamento de carga de servidores SIP para VoIP;

4.5.20.11. Permitir limitar o número de conexões estabelecidas com cada servidor real;

4.5.20.12. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;

4.5.20.13. Implementar Network Address Translation (NAT) do IP do servidor;

4.5.20.14. Implementar Network Address Translation (NAT) do IP do cliente;

4.5.20.15. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;

4.5.20.16. Implementar proteção contra SYN floods;

4.5.20.17. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;

4.5.20.18. 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;

4.5.20.19. Suportar Stream Control Transmission Protocol (SCTP);

4.5.20.20. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados assistida por hardware;

4.5.20.21. Permitir recriptografar a conexão entre a solução e o servidor;

4.5.20.22. Permitir espelhamento de tráfego de conexões TLS;

4.5.20.23. 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;

4.5.20.24. Em relação ao tráfego TLS, deve suportar:

4.5.20.24.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;

4.5.20.24.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;

4.5.20.24.3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve ser capaz de apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;

4.5.20.24.4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;

4.5.20.24.5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;

4.5.20.25. Suportar os algoritmos para sessões TLS:

4.5.20.25.1. SSL session cache Timeout;

4.5.20.25.2. Session Ticket;

4.5.20.25.3. OCSP (Online Certificate Status Protocol) Stapling;

4.5.20.25.4. Dynamic Record Sizing;

4.5.20.25.5. ALPN (Application Layer Protocol Negotiation);

4.5.20.25.6. Perfect Forward Secrecy;

4.5.20.26. Implementar limpeza de cabeçalho HTTP;

4.5.20.27. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;

4.5.20.28. 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;

4.5.20.29. 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;

4.5.20.30. Suportar log de todas as sessões, 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;

4.5.20.31. 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;

4.5.20.32. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

4.5.20.33. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

4.5.20.34. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga através dos serviços, modificando a configuração com base em mudanças feitas no ambiente;

4.5.20.35. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;

4.5.20.36. Permitir a configuração através de ConfigMaps e CustomResourceDefinition (CRD);

4.5.20.37. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods disponíveis para o serviço publicado;

4.5.21. Requisitos de proteção de aplicações no nível de rede e protocolo:

4.5.21.1. 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;

4.5.21.2. Proteger de ataques DDoS nas camadas de rede e de sessão, com mitigação assistida por hardware;

4.5.21.3. Proteger de ataques DDoS que utilizem SSL;

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

4.5.21.4.1. Endereço IP de destino;

4.5.21.4.2. Endereço IP de origem;

4.5.21.4.3. Porta de destino;

4.5.21.4.4. Porta de origem;

4.5.21.4.5. VLAN;

4.5.21.4.6. Protocolo;

4.5.21.4.7. Ação;

4.5.21.4.8. Horário;

4.5.21.4.9. Log;

4.5.21.4.10. Permitir definir agendamento para ativação da regra;

4.5.21.4.11. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;

4.5.21.5. Implementar a descoberta automática de serviços presentes em objetos monitorados;

4.5.21.6. Permitir definir, no mínimo, as seguintes ações no tráfego:

4.5.21.6.1. Permitir: os pacotes são aceitos e passam pelo firewall;

4.5.21.6.2. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;

4.5.21.6.3. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;

4.5.21.7. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:

4.5.21.7.1. Global, regras válidas para todo o tráfego;

4.5.21.7.2. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio;

4.5.21.7.3. Objeto, regras válidas para objetos específicos;

4.5.21.8. Deve possuir criptografia IPSec para comunicação entre sites;

4.5.21.9. 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;

4.5.21.10. Permitir a restauração das configurações de proteções originais;

4.5.21.11. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-rede;

4.5.21.12. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;

4.5.21.13. 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;

4.5.21.14. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;

4.5.21.15. Permitir a criação de regras de filtragem através de API REST declarativa, cuja documentação deve ser pública;

4.5.21.16. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito;

4.5.21.17. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;

4.5.21.18. 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 Fl SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;

4.5.21.19. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;

4.5.21.20. Limitar o número de consultas DNS por segundo através da configuração de limiares;

4.5.21.21. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflectio Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;

4.5.21.22. Suportar envio de SNMP traps para cada ataque DoS detectado;

4.5.21.23. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;

4.5.21.24. Deve possuir a funcionalidade de limiares automáticos para vetores de DoS. Essa funcionalidade deve valer tanto para proteção do equipamento como também para proteção de serviços específicos.

4.5.21.25. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;

4.5.21.26. 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;

4.5.21.27. Suportar integração com serviço de proteção de DDoS em nuvem, com compartilhamento de informação de vetores, através da sinalização de ataques em andamento para redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos, independente do provedor local de serviços de Internet;

4.5.22. Requisitos dos serviços de entrega de aplicações distribuídas através de DNS (GSLB)

4.5.22.1. Implementar serviços de DNS com as funções de DNS autoritativo, DNS secundário, DNS resolver, DNS cache e balanceamento de servidores de DNS;

4.5.22.2. Implementar DNSSEC, independente da estrutura dos servidores DNS em uso;

4.5.22.3. Implementar transferência de zonas para múltiplos servidores DNS primários responsáveis por diferentes zonas;

4.5.22.4. 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;

4.5.22.5. Implementar offload dos servidores de DNS, funcionando como o DNS secundário;

4.5.22.6. Implementar proteções contra-ataques DNS, incluindo validação de protocolo e floods;

4.5.22.7. Permitir a criação de códigos ou scripts que possam manipular as respostas de DNS;

4.5.22.8. Implementar filtragem de pacotes e tipos de requisições;

4.5.22.9. Implementar segurança do protocolo DNS, protegendo de ataques de negação de serviço, NXDOMAIN, reflexão e amplificação de DNS e Cache Poisoning;

4.5.22.10. Implementar stateful inspection das requisições e respostas de DNS;

4.5.22.11. Possuir base de geolocalização IP;

4.5.22.12. Implementar DNS64 e implementar as seguintes integrações:

4.5.22.12.1. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A e AAAA e responde com um prefixo + A e AAAA;

4.5.22.12.2. 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;

4.5.22.12.3. Cliente envia consulta AAAA, a solução encaminha uma consulta (recursivo) como A e responde um prefixo + AAAA.

4.5.22.13. Implementar filtros para tipos de requisição, de forma que apenas as operações e requisições autorizadas sejam encaminhadas para os servidores de DNS;

4.5.22.14. Suportar pelo menos os tipos de requisição SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV e TXT;

4.5.22.15. Suportar DNS over HTTPS (DoH);

4.5.22.16. Permitir a criação de resoluções de DNS com tratamento diferenciado de consultas conforme origem das requisições;

4.5.22.17. Apresentar estatísticas sobre consultas de DNS por aplicação, nome da consulta, tipo da consulta, endereço IP do cliente;

4.5.22.18. Implementar modo inline na estrutura de DNS existente e transparente;

4.5.22.19. Suportar IP Anycast;

4.5.22.20. Implementar alta disponibilidade sem depender de BGP ou outro protocolo de roteamento;

4.5.22.21. 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;

4.5.22.22. Suportar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde se originou a requisição;

4.5.22.23. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

4.5.22.24. Suportar monitores utilizando HTTP e HTTPS, incluindo a validação do SNI;

4.5.22.25. Suportar pelo menos os algoritmos de balanceamento Round Robin, Global Availability, Ratio, LDNS Persist, Geografia, round trip time e hops;

4.5.22.26. Implementar persistência da conexão do usuário entre aplicações ou data centers;

4.5.22.27. 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;

4.5.22.28. Permitir que as políticas sejam configuradas individualmente por aplicação que será balanceada;

4.5.22.29. Permitir que a contingência seja automática;

4.5.22.30. Permitir o retorno do Data Center de forma automática e manual;

4.5.22.31. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requisições AAAA);

4.5.22.32. Possuir suporte a IPv6 no balanceamento global entre datacenters;

4.5.22.33. Possuir a funcionalidade de resposta rápida a requisições de DNS, permitindo respostas mais rápidas para zonas que seja autoritativo;

4.5.22.34. 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 consultas DNS para domínios considerados maliciosos e retornar respostas customizadas;

4.5.22.35. Suportar EDNS-Client-Subnet (ECS) para tanto responder requisições de clientes para balanceamento de Data Center ou encaminhar requisições de clientes;

4.5.22.36. Implementar a utilização da subnet do cliente presente no ECS para tomada de decisão de balanceamento de Data Center, independente do endereço do LDNS;

4.5.22.37. Suportar inserir o ECS para outros servidores DNS;

4.5.22.38. 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;

4.5.22.39. 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;

4.5.22.40. 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;

4.5.22.41. Suportar, no mínimo, as ações de apenas registrar, bloquear o dado ou substituir o nome do domínio;

4.5.22.42. Permitir configurar limite de consultas (rate limit) realizadas via TCP ou UDP por FQDN;

4.5.22.43. Permitir configurar limite de consultas (rate limit) realizadas via TCP ou UDP por IP de origem;

4.5.23. Requisitos para proteção para aplicações web e API contra ameaças na camada de aplicação (WAF):

4.5.23.1. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;

4.5.23.2. Implementar ajustes automáticos e adaptativos de limiares de DoS;

4.5.23.3. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;

4.5.23.4. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;

4.5.23.5. Implementar modelo positivo de segurança de aplicações web;

4.5.23.6. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;

4.5.23.7. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;

4.5.23.8. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

4.5.23.9. 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;

4.5.23.10. Permitir a integração com firewall de banco de dados;

4.5.23.11. Suportar aplicações que utilizam protocolo WebSocket;

4.5.23.12. 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;

4.5.23.13. Implementar proteção contra:

4.5.23.13.1. Acesso por força bruta;

4.5.23.13.2. DoS e DDoS em camada 7;

4.5.23.13.3. Buffer Overflow;

4.5.23.13.4. Cross Site Request Forgery (CSRF);

4.5.23.13.5. Cross-Site Scripting (XSS);

4.5.23.13.6. Server-Side Request Forgery (SSRF);

4.5.23.13.7. SQL Injection;

4.5.23.13.8. Parameter tampering;

4.5.23.13.9. Cookie poisoning;

4.5.23.13.10. HTTP Request Smuggling;

4.5.23.13.11. Manipulação de campos escondidos (hidden input);

4.5.23.13.12. Manipulação de cookies;

4.5.23.13.13. Roubo de sessão através de manipulação de cookies;

4.5.23.13.14. Sequestro de sessão;

4.5.23.13.15. Validação de consistência de formulários;

4.5.23.13.16. Validação do cabeçalho do “User-Agent” para identificar clientes inválidos.

4.5.23.14. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);

4.5.23.15. Suportar codificação HTML "application/x-www-formurlencoded";

4.5.23.16. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;

4.5.23.17. Suportar codificação fragmentada (chunked encoding);

4.5.23.18. Suportar validações de protocolo:

4.5.23.18.1. Restrição de métodos;

4.5.23.18.2. Restrição de protocolos e versões;

4.5.23.18.3. Validação de conformidade com RFCs;

4.5.23.18.4. Validação de caracteres URL-encoded;

4.5.23.18.5. Validação de codificação fora de padrão %uXXYY.

4.5.23.19. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;

4.5.23.20. Suportar as técnicas de detecção:

4.5.23.20.1. URL-decoding;

4.5.23.20.2. Terminação Null Byte String;

4.5.23.20.3 .Paths autorreferenciados;

4.5.23.20.4. Case de caracteres misturados;

4.5.23.20.5. Uso excessivo de espaços em branco;

4.5.23.20.6. Decodificação de entidades HTML;

4.5.23.20.7. Caracteres de escape;

4.5.23.21. Suportar POST para upload de arquivo e permitir configurar restrições para tamanho individual de arquivo;

4.5.23.22. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);

4.5.23.23. Capacidade de filtrar cabeçalhos, corpo e status de respostas;

4.5.23.24. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

4.5.23.25. Implementar validação de URL;

4.5.23.26. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;

4.5.23.27. 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;

4.5.23.28 Suportar o uso de páginas de login que utilizam AJAX;

4.5.23.29. Permitir a customização da resposta de bloqueio;

4.5.23.30. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;

4.5.23.31. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;

4.5.23.32. Implementar as proteções:

4.5.23.32.1. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;

4.5.23.32.2. Ocultar qualquer mensagem de erro HTTP dos usuários;

4.5.23.32.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;

4.5.23.33. Permitir a configuração da página de bloqueio;

4.5.23.34. Suportar políticas por geolocalização para restrição de acesso a determinados países;

4.5.23.35. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;

4.5.23.36. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;

4.5.23.37. Implementar aprendizado automático de XML;

4.5.23.38. Permitir a importação de arquivo de esquema XML;

4.5.23.39. Implementar aprendizado automático de JSON;

4.5.23.40. Permitir a importação de arquivo de esquema JSON;

4.5.23.41. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;

4.5.23.42. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

4.5.23.43. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;

4.5.23.44. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;

4.5.23.45. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;

4.5.23.46. 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;

4.5.23.47. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;

4.5.23.48. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;

4.5.23.49. 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;

4.5.23.50. Possuir assinaturas de ataques para conteúdo em JSON e XML;

4.5.23.51. Possuir proteções contra XML Bomb;

4.5.23.52. 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;

4.5.23.53. 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;

4.5.23.54. 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, além de:

4.5.23.54.1. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

4.5.23.54.2. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;

4.5.23.54.3. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;

4.5.23.54.4. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;

4.5.23.54.5. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);

4.5.23.54.6. Implementar detecção com base no aumento de carga e processamento do servidor de aplicação;

4.5.23.54.7. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

4.5.23.55. 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;

4.5.23.56. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;

4.5.23.57. 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 e:

4.5.23.57.1. Identificar ataques com diferentes usuários e mesma origem;

4.5.23.57.2. Identificar ataques com diferentes origens e mesmo usuário;

4.5.23.57.3. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;

4.5.23.58. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;

4.5.23.59. 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;

4.5.23.60. 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;

4.5.23.61. Implementar detecção e mitigação para proteção contra bots contra robôs através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise comportamental;

4.5.23.62. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;

4.5.23.63. Implementar proteção proativa contra-ataques automatizados por bots e outras ferramentas, como web scrapers.

4.5.23.64. Possuir atualização automática de definição de bots;

4.5.23.65. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;

4.5.23.66. Permitir a criação de definições de bots;

4.5.23.67. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;

4.5.23.68. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;

4.5.23.69. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;

4.5.23.70. Permitir configurar exceções as regras de rate limits para chamadas na API;

4.5.23.71. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);

4.5.23.72. 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;

4.5.23.73. 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;

4.5.23.74. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;

4.5.23.75. 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;

4.5.23.76. 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;

4.5.23.77. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;

4.5.23.78. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;

4.5.23.79. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;

4.5.23.80. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;

4.5.23.81. Implementar um identificador único para cada requisição tratada pela solução;

4.5.23.82. Permitir o armazenamento local de eventos e exportação para servidores externos;

4.5.23.83. Permitir configurar a retenção dos eventos por tempo e volume;

4.5.23.84. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;

4.5.23.85. 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);

4.5.23.86. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;

4.5.23.87. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;

4.5.23.88. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;

4.5.24. Requisitos para as bases de inteligência de ameaças:

4.5.24.1. 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;

4.5.24.2. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiro homologado através de assinaturas de serviços próprios;

4.5.24.3. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;

4.5.24.4. 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;

4.5.24.5. 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;

4.5.24.6. 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;

4.5.24.7. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;

4.5.24.8. 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;

4.5.24.9. Deve dispor de bases de inteligência de sites, classificados e categorizados em, pelo menos, armazenamento e backup pessoal, compartilhamento de arquivos P2P, dados e serviços financeiros, colaboração, instituições culturais, instituições educacionais, organizações políticas, saúde e medicina, motores de busca, e-mail corporativo, endereços IP privados, produtividade, mensagens instantâneas, download de software, religião, redes sociais (Facebook, LinkedIn, Twitter e YouTube), websites recém cadastrados, sites com exposição elevada, conteúdo suspeito, explorações recentes, DNS dinâmico, prevenção de proxy, hacking, spam, lojas de aplicativos móveis não oficiais, sites comprometidos, sites maliciosos, phishing, fraudes, spyware e adware, keyloggers, software potencialmente indesejado, botnets, links malicioso, links suspeito, iFrame malicioso, malwares para dispositivos móveis, uploads criptografados ondemand, comando e controle;

4.5.24.12. 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;

4.5.24.13. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;

4.5.24.14. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;

4.5.24.15. 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;

4.5.24.16. 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.

4.5.25. Requisitos da solução de proteção de acesso a aplicações:

4.5.25.1. Deve permitir o controle de acesso a aplicações existentes baseado em políticas visuais (Visual Policy Editor);

4.5.25.2. Deve suportar autenticação multifator (MFA) com integração a RADIUS, LDAP, AD, SAML e OAuth;

4.5.25.3. Deve suportar autenticação baseada em certificados com verificação de CRL, OCSP e atributos;

4.5.25.4. Deve possuir suporte a portal de Acesso Seguro (SSL VPN / Application Portal) com as seguintes características:

4.5.25.4.1. Acesso via navegador (clientless) ou por agente (client-based) com suporte a SSL VPN;

4.5.25.4.2. Publicação de aplicações web e remotas por meio de portal customizável;

4.5.25.4.3. Suporte a tunelamento completo (full tunnel) ou por aplicação (per-app VPN);

4.5.25.4.4. Compatibilidade com múltiplos sistemas operacionais: Windows, macOS, Linux, iOS, Android;

4.5.25.4.5. Cliente VPN leve com distribuição automática via navegador;

4.5.25.4.6. Detecção de tipo de dispositivo e redirecionamento de políticas conforme o contexto (mobile, desktop, etc.);

4.5.25.5. Deve permitir a integração com sistemas de autenticação federada (SAML 2.0);

4.5.25.6. Deve oferecer suporte à verificação de integridade do dispositivo cliente (endpoint inspection) com suporte à verificação:

4.5.25.6.1. Do estado do antivírus;

4.5.25.6.2. Do estado do firewall;

4.5.25.6.3. Do estado atualização do sistema operacional;

4.5.25.6.4. Da presença de arquivos específicos;

4.5.25.6.5. Da existência de chaves de registro;

4.5.25.6.6. Da existência de determinados certificados instalados.

4.5.25.7. Deve possuir a capacidade de negar, redirecionar ou aplicar políticas diferenciadas com base nos resultados da inspeção;

4.5.25.8. Deve possuir a capacidade de aplicar políticas com base em dispositivo, rede, horário, localização e grupo;

4.5.25.9. Deve possuir suporte a APIs REST para automação e integração com SIEM;

4.5.25.10. Deve possuir a capacidade de encerrar sessões inativas automaticamente após tempo configurável;

4.5.25.11. Deve ser capaz de limitar a quantidade de sessões simultâneas por usuário;

4.5.25.12. Deve permitir o espelhamento de sessões entre equipamentos em alta disponibilidade para failover transparente;

4.5.25.13. Deverá oferecer funcionalidade de portal web seguro, que concentre o acesso remoto e interno a aplicações corporativas via navegador, com as seguintes características mínimas:

4.5.25.13.1. Acesso centralizado via portal HTML5 responsivo (compatível com navegadores modernos: Chrome, Firefox, Edge, Safari);

4.5.25.13.2. Capacidade de apresentar aplicações web, links internos, áreas de trabalho virtuais (VDI), pastas compartilhadas e recursos customizados por grupo de usuário;

4.5.25.13.3. Interface personalizável com logotipo da instituição, cores e identidade visual;

4.5.25.13.4. Exibição de aplicações com base em políticas (por grupo, IP, dispositivo, localização, horário, etc.);

4.5.25.13.5. Suporte a aplicações remotas como RDP, Citrix, VMware Horizon, com integração direta;

4.5.25.13.6. Suporte a Single Sign-On (SSO) para aplicações publicadas no portal;

4.5.25.13.7. Compatível com autenticação federada (ex: SAML 2.0) para autenticar usuários no acesso ao portal;

4.5.25.13.8. Mecanismos de proteção contra CSRF, XSS, e injeção de comandos;

4.5.25.13.9. Suporte a publicação de pastas e arquivos internos com controle de acesso;

4.5.25.13.10. Capacidade de incluir mensagens de aviso, banners e informações institucionais antes ou após o login;

4.5.25.13.11. Registro de acesso ao portal e suas aplicações, com logs auditáveis;

4.5.25.13.12. Compatível com múltiplos idiomas, incluindo português.

4.5.26. Requisitos de monitoramento da solução:

4.5.26.1. 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;

4.5.26.2. 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;

4.5.26.3. Suportar a exportação de eventos de DNS utilizando IPFIX;

4.5.26.4. Deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS;

4.5.26.5. Possuir relatório de ataques DDoS com indicação de início e fim do ataque;

4.5.26.6. Possuir relatório em tempo real sobre ataques DDoS, atualizado automaticamente;

4.5.26.7. Possuir relatório de ataques DDoS incluindo quantidade de eventos e severidade, ataques por protocolo, incluindo assinaturas utilizadas e serviços mais afetados;

4.5.26.8. Possuir relatórios de ataques DDoS incluindo a origem dos ataques, país, requisições por segundo, gatilho da proteção e mitigação adotada;

4.5.26.9. Suportar a exportação de eventos de DoS utilizando IPFIX;

4.5.26.10. Possuir painel de acompanhamento de adoção de proteções contra ameaças mais comuns, de acordo com OWASP Top 10 2021;

4.5.26.11. Possuir relatório de desempenho da solução, incluindo processamento total e por servidor virtual protegido;

4.5.26.12. 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;

4.5.26.13. Possuir relatório de incidentes com violações detectadas e correlacionadas, separando falsos positivos de atividades maliciosas e para facilitar a resposta a incidentes;

4.5.26.14. Implementar monitoração e análise de performance de aplicações web;

4.5.26.15. 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;

4.5.26.16. 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;

4.5.26.17. 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;

4.5.26.18. Possuir relatórios para análise de estatísticas de acesso, incluindo métodos HTTP, sistema operacional e navegadores;

4.5.26.19. Permitir exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário;

4.5.26.20. Possuir relatório de ataques DoS em camada 7 com indicação de início e fim do ataque;

4.5.26.21. Possuir relatório em tempo real sobre ataques DoS em camada 7, atualizado automaticamente;

4.5.26.22. Possuir relatório que permite avaliar o impacto de ataques DoS em camada 7 na performance do servidor;

4.6. Características específicas Item 2:

4.6.1 Fornecer subscrição de garantia e suporte com todas as funcionalidades descritas, operando com os limites de desempenho e conectividade especificados para o Item 1 (Appliance BIG IP R10900).

4.7. Características específicas Item 4:

4.7.1. Fornecer subscrição de garantia e suporte com todas as funcionalidades descritas, operando com os limites de desempenho e conectividade especificados para o Item 3 (Appliance BIG IP R5900).

4.8. Caracteristicas comuns aos serviços técnicos (Itens 5 e 6):

4.8.1 Deverão ser disponibilizados profissionais para a realização de atividades técnicas especializadas nas soluções contratadas nos itens 1 a 4, para realização de atividades como:

4.8.1.1. Definição/Validação de arquitetura; Análise de serviços inoperantes e troubleshooting;

4.8.1.2. Ajustes de configurações em softwares;

4.8.1.3. Implantação de alta disponibilidade e balanceamento de carga;

4.8.1.4. Implantação de processo de integração;

4.8.1.5. Atualização/Migração de versões;

4.8.1.6. Análise de performance do ambiente;

4.8.1.7. Documentação e repasse de conhecimento.

4.8.2. Os profissionais designados para a execução dos serviços técnicos deverão ser do fabricante e possuir certificações válidas, de acordo com os produtos e serviços envolvidos na respectiva Ordem de Serviço;

4.8.3. A Hora de Serviço Técnico é a unidade de medida utilizada para dimensionar o custo e remunerar o provedor de serviços, cujo escopo de avaliação deverá sempre estar vinculado aos resultados apresentados (entregáveis específicos de cada pacote de serviço) e ao cumprimento de níveis mínimos de serviço atrelados;

4.8.4. Em nenhuma hipótese haverá remuneração do provedor meramente com base nas horas de serviço empenhadas em determinado processo (ou pacote de serviço) de forma desvinculada da entrega de resultados e/ou entrega de valor. Assim como, não haverá remuneração por serviços executados não demandados ou não especificados nas demandas;

4.8.5 . Cada pacote de serviços será composto por 4 horas de atividade do profissional.

4.9. Características específicas aos serviços técnicos Standard (Item 5):

4.9.1. Os serviços serão prestados remotamente durante o horário comercial padrão definido como segunda a sexta-feira, das 8h às 18h (horário de Brasília), exceto feriados nacionais.

4.9.2 O acionamento e agendamento dos serviços deverão ocorrer com antecedência mínima de 5 (cinco) dias úteis, através dos canais oficiais designados pela CONTRATADA.

4.10. Características específicas aos serviços técnicos Premium (Item 6):

4.10.1. Os serviços poderão ser prestados remotamente fora do horário comercial padrão (noites, fins de semana e feriados nacionais), conforme necessidade da CONTRATANTE.

4.10. 2 O acionamento e agendamento dos serviços deverão ocorrer a qualquer momento, em regime emergencial, com objetivo de obter apoio técnico para o reestabelecimento de serviços.

4.11. Características comuns aos treinamentos (Item 7 e Item 8):

4.11.1. O objetivo do serviço de treinamento é habilitar os participantes a configurar, operar e administrar/gerenciar os produtos especificados neste documento;

4.11.2. O treinamento deverá ser oficial do fabricante;

4.11.3. O treinamento deverá ser ministrado preferencialmente na língua portuguesa, por instrutores de comprovada experiência técnica e didática;

4.11.4.Os instrutores deverão possuir certificação do Fabricante, da solução ofertada, para prestar serviço de treinamento;

4.11.5. Deverá ser fornecida, no início do treinamento, material de acompanhamento com todo o seu conteúdo programático, para cada participante;

4.11.6. Deverá ser fornecido certificado de participação, após cada treinamento, para cada participante que obtiver presença mínima de 90% (noventa por cento);

4.11.7. O treinamento deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente. O conteúdo abordado deve apresentar, de forma teórica e prática, as características técnicas que envolvem os produtos adquiridos, demonstrando como configurá-los de acordo com a arquitetura, as necessidades e as peculiaridades do ambiente operacional da CONTRATANTE;

4.11.8. A CONTRATANTE poderá solicitar a repetição do treinamento caso entenda que os requisitos estipulados não foram cumpridos, por ato devidamente motivado, oportunizando a manifestação da empresa, em atendimento ao dever de motivação do ato administrativo (art. 2º da Lei Estadual nº 13.800/2001), bem como ao princípio do devido processo legal (art. 5º, inciso LIV da CF).

4.11.9. Após o término da carga horária do treinamento, a equipe técnica participante receberá um questionário, por meio de ficha de avaliação a ser disponibilizada pelo CONTRATANTE, onde serão avaliados os seguintes aspectos:

4.11.9.1. Se a metodologia de ensino do instrutor e seu grau de conhecimento sobre o assunto estão de acordo com as exigências deste Termo de Referência e seus Anexos e com o grau de complexidade e de responsabilidade exigidos por essa contratação;

4.11.9.2. Se o treinamento atingiu as expectativas de ganho de conhecimento esperada pelos participantes;

4.11.9.3. e as condições físicas do local/sala de aula eram de boa qualidade.

4.11.10. Caso a avaliação média do treinamento seja inferior a 3 (três), de um total de 4 (quatro) pontos, a CONTRATADA deverá realizar novo treinamento, conforme novo cronograma a ser estabelecido entre as partes, sem ônus, e com as reformulações que a CONTRATANTE entender necessárias;

4.11.11. O treinamento pode ser realizado presencial ou remoto, atendendo os seguintes requisitos:

4.11.11.1. Para o treinamento presencial o local deverá ser disponibilizado pela CONTRATADA, na cidade Goiânia, devendo todos os custos (sala, instrutores, desktops, ferramental, etc.) ser de responsabilidade da mesma;

4.11.11.2. O treinamento não presencial (treinamento à distância ou remoto) deve atender a todos os requisitos solicitados neste item e obrigatoriamente deve ser ministrado com a presença online do instrutor e do treinando.

Tópico 5 - FUNDAMENTAÇÃO DA CONTRATAÇÃO

5.1. A presente contratação de Fornecimento de Bens e Materiais e Serviços - Expansão de Solução de Application Delivery Controller (ADC) está fundamentada nos termos do [ETP - Estudo Técnico Preliminar].

5.2. A Subsecretaria de Tecnologia da Informação do Estado de Goiás (STI/GO) desempenha papel estratégico na modernização da administração pública, provendo soluções tecnológicas que garantem eficiência, disponibilidade e segurança dos sistemas governamentais. Com o crescimento contínuo da demanda por serviços digitais, a infraestrutura atual de entrega de aplicações requer ampliação para manter níveis adequados de desempenho, confiabilidade e segurança.

5.3. O Application Delivery Controller (ADC) é um componente essencial da arquitetura de TI, atuando no balanceamento de carga, aceleração de aplicações, segurança de dados e alta disponibilidade de serviços. Atualmente, a solução em uso encontra-se próxima de seu limite de capacidade, o que compromete o desempenho e a escalabilidade de sistemas críticos, como:

5.3.1. Portais de atendimento ao cidadão (ex: Detran, Saúde, Educação);

5.3.2. Sistemas de gestão administrativa e financeira do Estado;

5.3.3. Ambientes de serviços em nuvem e integrações com APIs governamentais.

5.4 Objetivos da Expansão:

5.4.1 A expansão da solução ADC tem como principais objetivos:

5.4.1.1. Aumentar a capacidade de balanceamento de carga, suportando um maior volume de acessos simultâneos;

5.4.1.2. Reduzir a latência e melhorar o tempo de resposta das aplicações, otimizando a experiência do usuário;

5.4.1.3. Reforçar a segurança no tráfego de dados, com recursos avançados de inspeção de pacotes, mitigação de ataques (ex: DDoS, injeção de código) e controle de acesso;

5.4.1.4. Garantir alta disponibilidade e tolerância a falhas, minimizando o risco de interrupção dos serviços públicos digitais;

5.4.1.5. Apoiar a transformação digital e a adoção de novas tecnologias, como microserviços, containers e arquiteturas em nuvem híbrida.

5.5. Benefícios Esperados:

5.5.1. Melhoria da eficiência operacional, com menor tempo de inatividade e menor necessidade de intervenções manuais;

5.5.2. Redução de custos a médio prazo, ao evitar colapsos de sistema e indisponibilidades que geram retrabalho e perda de produtividade;

5.5.3. Maior segurança da informação, em conformidade com a LGPD e outras normas de governança digital;

5.5.4. Melhor atendimento ao cidadão, com serviços online mais rápidos, estáveis e seguros.

5.6. Conclusão

5.6.1. A aquisição da expansão da solução de Application Delivery Controller (ADC) é estratégica para garantir a continuidade e evolução dos serviços digitais do Governo do Estado de Goiás. Trata-se de um investimento essencial para suportar o crescimento da demanda, promover a inovação tecnológica e assegurar a qualidade e segurança das aplicações públicas.

Tópico 6 - REQUISITOS DA CONTRATAÇÃO

6.1. O objeto da contratação deve seguir todos os requisitos e padrões regionais ou nacionalmente estabelecidos.

Da exigência de carta de solidariedade

6.2. Em caso de fornecedor, revendedor ou distribuidor, **não** será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

6.2.1. Entretanto, como critério de aceitabilidade da proposta de preços, deverá ser apresentada a comprovação de que é revendedora ou distribuidora credenciada pelo fabricante para comercializar seus produtos no território nacional, devendo possuir a habilitação como revendedor autorizado no Brasil.

6.2.2. A habilitação de que trata o item anterior não se trata de um requisito de qualificação, mas de um título habilitante (de base contratual entre fabricante e revendedor) consistente em um critério de aceitabilidade da proposta provisoriamente classificada em primeiro lugar.

6.2.3. A verificação poderá ser através de declaração nominal emitida pelo fabricante, ou através da página oficial do fabricante.

6.2.4. Ainda, sobre a exigência de comprovação de credenciamento junto ao fabricante, este requisito busca garantir a aquisição adequada de produtos e licenças do fabricante, mitigando os riscos associados ao fornecimento de licenças não oficiais ou com suporte inadequado por parte do fabricante. Além disso, essa medida confirma que a empresa fornecedora possui as competências e habilidades necessárias para fornecer os produtos e serviços associados, garantindo que as organizações tenham acesso a um suporte eficiente, atualizações regulares e recursos de segurança robustos, que são cruciais para a operação contínua e segura dos sistemas e ambientes baseados nos produtos contratados.

Da Declaração de Não Ocorrência de Registro de Oportunidade

6.3. Como critério de aceitabilidade da proposta de preços, deverá ser apresentada pela licitante provisoriamente classificada em primeiro lugar, documento denominado "**Declaração de Não Ocorrência de Registro de Oportunidade**", que consiste em uma declaração do licitante que ateste a não ocorrência do registro de oportunidade junto ao fabricante da solução, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, conforme disposto na Lei nº 14.133, de 2021.

6.3.1. Considerando que a contratação trata-se de subscrição de licenças de uso de *software* de fabricante único, a existência do Registro de Oportunidade possui viés

anticompetitivo, já que desestimula a participação dos demais revendedores do mesmo fabricante.

6.3.2. Esse cenário leva à realização de licitações com falsa competição, pois o revendedor que possui o registro de oportunidade oferece o menor preço e os demais participam do certame como figurantes.

6.3.3. Desta forma, a exigência de apresentação da "**Declaração de Não Ocorrência de Registro de Oportunidade**" implica em respeito às regras concorrenciais e competição saudável no mercado, além de cumprimento aos princípios da economicidade e competividade previstos pela legislação vigente, não estabelecendo qualquer restrição à concorrência ou participação em certames, mas sim a ampla concorrência.

Indicação de marcas ou modelos

6.4. Na presente contratação, a indicação de marca, características ou modelo específicos é admitida e tecnicamente justificada, primariamente pela **necessidade de padronização** e manutenção da **compatibilidade com a infraestrutura tecnológica já implantada e consolidada** no âmbito da Administração Pública Estadual.

6.4.1. Tal prerrogativa encontra amparo na **Súmula nº 270 do Tribunal de Contas da União (TCU)**, que estabelece:

> *"Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação".*

6.5. A decisão de indicar uma marca específica, neste caso, não visa restringir a competitividade, mas sim atender a um imperativo técnico e administrativo de otimização de recursos e garantia da interoperabilidade.

6.6. No contexto da Administração Pública Estadual, a solução de Controle de Entrega de Aplicações (ADC) com Web Application Firewall (WAF) do fabricante F5, modelo BIG-IP, já se encontra com uso sedimentado e integrado aos sistemas e serviços críticos do Estado. A presente contratação visa, portanto, assegurar a continuidade operacional, a manutenção da compatibilidade e o aproveitamento dos investimentos já realizados, bem como da expertise técnica já desenvolvida internamente.

6.7. Essa estratégia de padronização é fundamental para:

Garantir a interoperabilidade com os demais componentes da infraestrutura existente, evitando conflitos técnicos e degradação de performance.
Mitigar riscos e custos associados à migração para uma nova plataforma (incluindo reconfiguração de serviços, treinamento de equipes e potencial indisponibilidade durante a transição).
Otimizar a gestão e o suporte técnico, concentrando esforços em uma plataforma conhecida e dominada pela equipe técnica.
Assegurar a uniformidade dos níveis de serviço e segurança já estabelecidos.

6.8. Esta abordagem está em plena consonância com os princípios da eficiência administrativa e com o disposto na Lei nº 14.133/2021, notadamente em seu **art. 40, inciso V, alínea "a"**, que orienta o planejamento de contratações para considerar a padronização, e no **art. 41, inciso I**, que permitem a indicação de marca em decorrência da necessidade de padronização do objeto ou da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração, desde que devidamente justificado.

Garantia da contratação

6.9. Será exigida a garantia da contratação de que trata o art. 96, da Lei federal nº 14.133, de 01 de abril de 2021

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

6.10.1. O prazo de vigência da apólice será igual ou superior ao prazo estabelecido no contrato principal e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora.

6.11. Em caso de opção de garantia, nas modalidades caução ou fiança bancária, esta deverá ser prestada em até 10 (dez) dias úteis após a assinatura do contrato.

Obrigações pertinentes à Lei Geral de Proteção de Dados Pessoais (LGPD)

6.12. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão da licitação ou da contratação, a partir da apresentação da proposta no certame, independentemente de declaração ou de aceitação expressa.

6.13. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

6.14.É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

6.15.A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

6.16. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do Contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

6.17.É dever do Contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

6.18.O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

6.19.O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

6.20.O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

6.21. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

6.22.O presente instrumento está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD, por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

6.23. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

Tópico 7 - MODELO DE EXECUÇÃO DO OBJETO

O objeto contratado deverá ser entregue ou prestado mediante o cumprimento das seguintes condições:

Prazos e locais de entrega:

7.1. O prazo de entrega, instalação e configuração da solução, referente aos itens é de até 60 (sessenta) dias corridos após a emissão da ordem de fornecimento;

7.2. Os equipamentos deverão ser entregues e instalados nos Data Centers Corporativos do Governo do Estado de Goiás (DC1 e DC2) localizados nos endereços abaixo:

DC1	Av. Ver. José Monteiro, 2233 - Nova Vila, Goiânia - GO, 74653-900

7.2.1. O horário de entrega de bens será das 08:00h às 12:00h e das 13:00h às 17:00h em dias úteis, conforme horário de Brasília. Não serão recebidos produtos fora deste horário, salvo prévio acordo;

7.3. O prazo de entrega dos serviços será definido na Ordem de Serviço ou Fornecimento, emitida pelo Gestor e/ou Fiscal do Contrato.

7.4. Com relação aos equipamentos, os mesmos deverão ser de primeira qualidade, de primeiro uso, transportados e acondicionados de maneira que garanta sua integridade, acompanhados de manual do usuário em português, na forma, quantidade e prazos previstos no Instrumento Contratual e no Termo de Referência, que integram o Edital;

7.5 Quando cabível, os produtos a serem entregues devem ser acondicionados em embalagem apropriada, de forma segura, com os respectivos acessórios, com marca, manual e modelo impressos.

7.6. Com relação aos softwares, os mesmos deverão ser entregues em formato eletrônico (CD ou DVD) ou podem ser disponibilizados através de portal web do fabricante do software, desde que sejam providos mecanismos de controle de acesso e integridade apropriados;

7.7. Os pedidos de prorrogação de prazo de entrega só serão examinados quando formulados à CONTRATANTE até o prazo limite de entrega;

7.8. Os itens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo Fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades;

Cronograma de execução:

7.9. A execução do objeto contratado seguirá o seguinte cronograma físico-financeiro:

CRONOGRAMA FÍSICO-FINANCEIRO		
Seq.	**Descrição**	**Prazo**
1	Assinatura do Contrato	-
2	Emissão da Ordem de Serviço / Fornecimento para o Item de Contratação 01 - Subscrição de Licenças	Imediatamente após a Assinatura do Contrato.
3	Reunião Inicial de *Kick-Off*	Até 05 (cinco) dias corridos após a Assinatura do Contrato.
4	Entrega dos Itens de contratação 01 ao 04	Até 60 (dias) dias corridos após emissão da Ordem de Serviço / Fornecimento.
5	Pagamento integral dos itens de contratação 01 e 03	Até 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo das Licenças e Ateste da Nota Fiscal.
6	Pagamento - 1° Parcela Anual dos Itens de contratação 02 e 04	Até 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo e Ateste da Nota Fiscal.
7	Entrega dos Serviços Técnicos (Itens de Contratação 05 e 06)	Em cronograma a ser definido pela CONTRATANTE
8	Pagamento dos Serviços Técnicos (Itens de Contratação 05 e 06)	Até 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo do Serviço de Implantação e Ateste da Nota Fiscal.
9	Realização do Treinamento Oficial (Itens de Contratação 07 e 08)	Em cronograma a ser definido pela CONTRATANTE
10	Pagamento do Treinamento Oficial (Itens de Contratação 07 e 08)	Até 30 (trinta) dias corridos após a emissão do Termo de Recebimento Definitivo do Treinamento Oficial e Ateste da Nota Fiscal.
11	Pagamento - 2° Parcela Anual dos Itens de contratação 02 e 04	12 (doze) meses após a emissão do Termo de Recebimento Definitivo das Licenças e Ateste da Nota Fiscal.
12	Pagamento - 3° Parcela Anual dos Itens de contratação 02 e 04	24 (vinte e quatro) meses após a emissão do Termo de Recebimento Definitivo das Licenças e Ateste da Nota Fiscal.

7.10. Caso não seja possível a entrega na data determinada, a empresa deverá comunicar as razões respectivas com pelo menos 10 dias de antecedência para que qualquer pleito de prorrogação de prazo possa ser analisado, ressalvadas situações de caso fortuito e força maior.

7.11. A Lei nº 4.320/64 afirma que "o pagamento da despesa só será efetuado quando ordenado após sua regular liquidação" (art. 62). A referida norma também determina que a liquidação da despesa terá por base, dentre outros documentos, os comprovantes de entrega de material ou da prestação efetiva do serviço. Portanto, podemos inferir que o pagamento da despesa somente pode ocorrer após a comprovação da entrega do material ou da prestação efetiva do serviço.

7.12. Conforme entendimento do Tribunal de Contas da União, sedimentado através do Acórdão 2569/18 - TCU (https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/NUMACORDAO%253A2569%2520ANOACORDAO%253A2018/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/sinonimos%253Dfalse), no caso de licenças de software, o momento da entrega definitiva é o da ativação da licença.

7.13. Assim sendo, considerando que o Termo de Recebimento Definitivo se dará somente após a ativação das licenças, o pagamento aqui descrito não se configura em antecipação.

Garantia, manutenção e suporte técnico e Níveis minimos de Serviços (NMS):

7.14. Todos os equipamentos e softwares descritos nesta especificação devem possuir garantia e suporte do próprio Fabricante do Equipamento ou do Desenvolvedor do Software por um período mínimo de 60 (sessenta) meses. O suporte deverá ser prestado pela CONTRATADA e pelo Fabricante do Equipamento/Desenvolvedor do Software, também por um período mínimo de 60 (sessenta) meses;

7.15. A garantia e suporte técnico para os componentes da solução tem natureza de serviço contínuo, pois há a manutenção de um produto ou prestação de informações de uso, não havendo necessidade de o produto apresentar qualquer defeito para que o serviço seja prestado. Cabe ressaltar que o suporte técnico tem característica de ser do tipo help desk, em caráter contínuo, inclusive para apoio e saneamento de dúvidas na utilização dos equipamentos (hardwares) ou programas (softwares). Importante destacar que há inclusive definição de níveis mínimos de atendimento para acionamento do suporte e garantia e que o não atendimento nos prazos definidos poderá ensejar penalidades à Contratada.

7.16. A garantia e suporte técnico, compreende a assistência técnica ininterrupta, com atendimento 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e, se necessária, deverá ser prestada na modalidade de atendimento local on-site, isto é, nas dependências onde estiverem instalados os equipamentos, englobando o objeto entregue, considerando o firmware, hardware, placas de rede, módulos, peças, serviços, manutenção preventiva, manutenção corretiva, manutenção evolutiva, atualização de software do produto sempre que a fabricante disponibilizar nova versão de atualização, compreendendo ainda defeitos decorrentes de projeto, fabricação, construção, montagem ou acondicionamento, orientação sobre a utilização e configuração dos softwares e hardware que compõe o objeto, PELO PERÍODO MÍNIMO DE 60 (sessenta) MESES A CONTAR DA DATA DO RECEBIMENTO DEFINITIVO do objeto;

7.17. Manutenção preventiva é o conjunto de ações efetuadas em intervalos predeterminados, ou de acordo com critérios prescritos pelo fabricante ou boas práticas, destinadas a reduzir a probabilidade de falha ou a degradação do funcionamento de um item;

7.18. Manutenção corretiva é aquela destinada a identificar e corrigir os defeitos apresentados no hardware ou software e deverá ocorrer em todas as ocasiões que demandado pelo CONTRATANTE ou naquelas que forem detectadas pela CONTRATADA em suas ações de manutenção preventiva;

7.19. Manutenção evolutiva é o fornecimento de novas versões e/ou releases corretivas e/ou evolutivas de softwares lançadas durante a vigência da garantia contratual, mesmo em caso de mudança de designação do nome do software. A cada nova liberação de versão e release, a Prestadora de Serviço deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem. Inclui também, implementações de novas funcionalidades relativas aos equipamentos ou ao software de acordo com o interesse da CONTRATADA;

7.20. Durante todo o período de garantia e suporte, não haverá limites para quantidade de abertura dos chamados técnicos para hardwares: substituição de equipamentos ou de peças defeituosas por itens novos e de primeiro uso, atualizações de firmwares, bem como outros componentes pertinentes;

7.21. A não correção preventiva de alguma falha que tenha sido detectada pela CONTRATADA antes do seu agravamento, será caracterizada como negligência e estará passível a aplicação de penalidades;

7.22. As atividades de manutenção preventiva, corretiva ou evolutiva deverão ser realizadas preferencialmente por técnicos do fabricante devidamente certificados e autorizados;

7.23. Serão permitidas a realização de manutenção preventiva, corretiva ou evolutiva por técnicos da CONTRATADA devidamente certificados e autorizados pelo fabricante, devendo nesta situação a CONTRATADA ser parceira, representante ou autorizada técnica do fabricante na solução com autorização para executar manutenções;

7.24. A garantia e o suporte de toda a solução deverá respeitar os períodos estipulados (tendo o início da contagem após 1 (um) dia útil da emissão do Termo de Recebimento Definitivo) e ser emitida em nome da CONTRATANTE, sendo devidamente comprovada através de documentação emitida pelo fabricante da solução de Hardware/Software;

7.25. Durante o prazo de garantia e suporte técnico, será substituída, sem ônus para a Contratante, a parte ou peça defeituosa, salvo quando o defeito for provocado por uso inadequado dos equipamentos;

7.26. Deverá ser disponibilizada Central de Atendimento (0800) e/ou Web site em Português do Brasil para abertura e acompanhamento dos chamados de garantia e suporte técnico, comprometendo-se a manter seus registros e descrições completas;

7.27. O serviço de suporte compreende a abertura de chamados 24x7, ou seja, vinte e quatro horas por dia, sete dias por semana;

7.28. Para os chamados de qualquer severidade, a critério da CONTRATANTE, poderá ser agendado o melhor horário para atendimento;

7.29. Ao final de cada atendimento, é obrigatória a apresentação de relatório contendo as informações de data e hora da realização das atividades, nome do responsável pela demanda, nome do responsável pelo atendimento, número de controle (protocolo) e descrição sucinta do serviço;

7.30. A CONTRATANTE poderá acionar o suporte técnico da CONTRATADA para contar com o apoio para realização de planejamento e configurações de novos serviços que envolvam a solução, aplicação de updates das versões de software nos equipamentos, acompanhamento de janelas de manutenção programadas em qualquer horário e troubleshooting de redes;

7.31. A substituição de peças ou componentes mecânicos ou eletrônicos deverá sempre utilizar produtos novos e originais da mesmas homologados pelo fabricante da solução;

7.32. Caso seja impossível a recuperação do equipamento que apresentou o problema, a CONTRATADA deverá fornecer em substituição ao defeituoso outro equipamento idêntico ou superior, novo e de primeiro uso, definitivamente, em substituição do defeituoso, em prazo não superior a 10 (dez) dias;

7.33. A CONTRATADA deverá substituir o equipamento ou componente já instalado por um novo, sem ônus para a CONTRATANTE, caso ocorram 3 (três) ou mais defeitos que acarretem em indisponibilidade total do mesmo equipamento ou componente, dentro de qualquer intervalo de 30 (trinta) dias;

7.34. A CONTRATADA deverá disponibilizar acesso ao conteúdo do site do fabricante, ao contrato de suporte, às atualizações de releases e versões, à base de conhecimento incluindo sintomas conhecidos e soluções propostas e às especificações e literatura técnica;

7.35. Caso o modelo de equipamento ou componente não seja mais disponibilizado pelo fabricante, a CONTRATADA poderá fornecer equipamento ou componente similar, com características iguais ou superiores ao equipamento original, mediante aprovação por parte do gestor do contrato;

7.36. Durante o período de garantia a CONTRATADA fornecerá a CONTRATANTE, sem ônus adicional, quaisquer atualizações ou recalls disponibilizadas pelo fabricante para os softwares que compõe a solução contratada, ficando responsável pela instalação, mediante prévia anuência do CONTRATANTE;

7.37. A CONTRATANTE deverá ter a opção de abrir Ordem de Serviço diretamente a CONTRATADA ou fabricante, caso em que os prazos de atendimento ao chamado serão aqueles definidos pelo serviço de suporte do próprio fabricante, desde que seja mais vantajoso para a CONTRATANTE;

7.38. Dos requisitos de manutenção preventiva:

7.38.1. Os serviços compreendem verificações com relação ao bom funcionamento do hardware e à atualização de softwares e firmwares necessários para todos os itens que compõem os equipamentos listados no objeto;

7.38.2. A data da realização das manutenções preventivas deverá ser acorda entre CONTRATADA e CONTRATANTE;

7.38.3. A futura CONTRATADA deverá realizar a manutenção preventiva, realizando:

7.38.3.1. Análise de logs e configurações da solução, identificando possíveis erros ou conflitos e as correções necessárias;

7.38.3.2. Análise de desempenho do funcionamento da solução no que diz respeito ao uso de CPU e memória e recomendar ajustes;

7.38.3.3. Análise física dos equipamentos, incluído verificações de temperatura, ventilação e eventuais alertas de falhas de hardwares;

7.38.3.4. Análise de vulnerabilidades e de pendências de atualizações de versões de firmwares, engines, assinaturas ou qualquer componente da solução passível de atualização e recomendar as ações necessárias para regularização;

7.38.3.5. Durante toda a vigência contratual, a CONTRATADA deverá fornecer à equipe técnica da CONTRATANTE todas as informações referentes a novas versões do produto lançadas no mercado, orientando a CONTRATANTE para, quando lhe for conveniente, proceder à aplicação de pacotes de correção e migração de versões do produto;

7.38.3.6. Os serviços de manutenção preventiva não constituem serviços de consultoria especializada, exceto quando solicitada manutenção em período diferente do previsto.

Níveis Mínimos de Serviço Exigidos (NMS):

7.39. Os prazos máximos para a solução dos chamados de manutenção corretiva, de acordo com o nível de severidade de cada chamado, são:

Severidade do Incidente	Cenários	Prazo de início do Atendimento	Prazo de solução	Multa por descumprimento
Alto Impacto	Parada total da solução - mecanismos de contingência não funcionam; indisponibilidade total ou parcial das instâncias de um cluster no sítio; indisponibilidade total de um ou mais serviços das instâncias que compõem um sítio; degradação de serviços providos pelas instâncias que compõem o sítio; indisponibilidade ou degradação no mecanismo de balanceamento	1 (uma) hora	4 (quatro) horas	0,05% nas 8 primeiras horas; 0,10% nas horas seguintes.

	entre os sítios.			
Médio impacto	Aqueles para os quais houver solução de contorno cujo impacto não comprometa a operação dos serviços que utilizam a solução.	Próximo dia útil	7 (sete) dias	Penalidades prevista no Título SANÇÕES ADMINISTRATIVAS da minuta de contrato. Penalidades prevista no Título SANÇÕES ADMINISTRATIVAS da minuta de contrato.
Baixo Impacto	Aqueles que não afetem o perfeito funcionamento da solução.	Próximo dia útil	30 (trinta) dias	
Externo	Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela Contratada. Neste caso, ficam suspensos todos os prazos de atendimento até que o Contratante resolva os problemas externos que provocam a inoperância da solução.	Após disponibilizar o ambiente de forma estável para a reativação da solução, a Contratada realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.		

7.39.1. O prazo de solução é o tempo máximo requerido para que o serviço ou sistema impactado volte a funcionar, independentemente de ter sido resolvida a causa raiz do problema;

7.39.2. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

7.39.3. O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.

7.39.4. O atendimento das severidades de "Alto Impacto" deverá ser prestados de forma ininterrupta, ainda que o prazo para solução do problema avance sobre dia não útil;

7.39.5. O atendimento das severidades de impacto Médio, Baixo e Externo" descritos na Tabela poderão ser transferidos para o próximo dia útil caso o prazo para solução do problema alcance dia não útil;

7.39.6. Caberá exclusivamente à CONTRATANTE a definição da severidade do chamado técnico;

7.39.7. As intervenções que possam causar indisponibilidades devem ser executadas em horários definidos pela CONTRATANTE;

7.40. O indicador de atraso de entrega está indicado abaixo:

INDICADOR DE ATRASO NA ENTREGA (IAE)	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes nas Ordens de Serviço ou Fornecimento.
Meta a cumprir	IAE <=0 (A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço ou Fornecimento dentro do prazo previsto.)
Instrumento de medição	Ordem de Serviço ou Fornecimento, Termo de Recebimento Provisório e Definitivo.
Forma de acompanhamento	A avaliação será realizada por meio da verificação da data de entrega constante na Ordem de Serviço ou Fornecimento e da data de recebimento provisório das licenças.
Periodicidade	Por Ordem de Serviço ou Fornecimento
Mecanismo de Cálculo (métrica)	TEX = (DEE - DDE) Onde: TEX = Tempo de execução (quantidade de dias entre o envio da Ordem de Serviço ou Fornecimento e o recebimento provisório). DDE = Data definida para entrega das licenças constante na Ordem de Serviço ou Fornecimento. DEE = Data efetiva da entrega das licenças.
Faixas de ajuste no pagamento e glosas	Para valores iguais ou inferiores a 0 (zero) dia: Pagamento integral do valor da parcela de fornecimento; Para valores acima a 0 (zero) dia: 0,1% (zero vírgula um por cento) de glosa por dia útil de atraso, sobre o valor da Ordem de Serviço ou Fornecimento.

7.41. As glosas poderão ser descontadas dos pagamentos devidos, dos valores a serem pagos nas próximas parcelas anuais, ou serem cobradas diretamente da CONTRATADA.

7.42. A glosa é uma medida de controle administrativo, com repercussão financeira mas sem natureza sancionatória, que consiste no ajuste ou retenção de valores devidos à CONTRATADA quando o serviço não é prestado conforme os níveis de serviço acordados.

7.43. Quando a responsabilidade da resolução de chamado ou solução de contorno recair exclusivamente para o fabricante da solução, referente a problemas cuja solução dependa de correção de falhas (*bugs*) ou da liberação de novas versões e *patches* de correção, não haverá responsabilização da empresa CONTRATADA, considerando que o atraso na execução do objeto deriva de conduta não atribuível diretamente à ela.

Tópico 8 - MODELO DE GESTÃO DO CONTRATO

Responsabilidade do Fornecedor

8.1. Não obstante o Fornecedor ser o único responsável pela entrega do objeto ou prestação de serviço, a Administração se reserva no direito de exercer a mais ampla e completa fiscalização sobre o fornecimento ou prestação de serviço, nos termos da legislação aplicável.

8.2. O Fornecedor será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pela Administração.

Comunicação

8.3. As comunicações entre o órgão ou entidade e o Fornecedor serão realizadas por escrito, admitindo-se o uso de notificação ou mensagem eletrônica registrada no sistema SISLOG destinada a esse fim, realizadas pelo Gestor do Contrato, ou seu respectivo substituto, formalmente designado.

Reunião inicial do contrato

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

Registro de Ocorrências

8.5. Serão registradas todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

Gestão e fiscalização do contrato

8.6. O contrato será acompanhado pelo Gestor e Fiscal do Contrato, ou seus respectivos substitutos, formalmente designados nos termos do Decreto estadual n° 10.216,

de 14 de fevereiro de 2023, responsáveis pela fiscalização, acompanhamento e verificação da perfeita execução contratual, em todas as fases até a finalização do contrato.

8.7. O Gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato e será responsável pela comunicação com representantes do Fornecedor, nos termos do art. 22 do Decreto estadual n° 10.216, de 14 de fevereiro de 2023.

8.8. O Gestor do contrato coordenará as atividades relacionadas à fiscalização técnica, administrativa e setorial, aos atos preparatórios à instrução processual e encaminhará a documentação pertinente ao setor de contratos para a formalização dos procedimentos relativos à alteração, prorrogação ou rescisão contratual ou para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções.

Fiscalização Técnica

8.9. O Fiscal Técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração, segundo suas atribuições descritas no art. 23 do Decreto estadual n° 10.216, de 14 de fevereiro de 2023.

8.10. O Fiscal Técnico acompanhará o contrato com o objetivo de avaliar a execução do objeto nas condições contratuais e, se for o caso, aferir se a quantidade, a qualidade, o tempo e o modo da prestação ou da execução do objeto estão compatíveis com os indicadores estabelecidos no edital para o pagamento, com possibilidade de solicitar o auxílio ao Fiscal Administrativo ou Setorial, e ainda informar ao gestor do contato, em tempo hábil, a ocorrência relevante que demandar decisão ou adoção de medidas que ultrapassem sua competência ou a existência de riscos quanto à conclusão da execução do objeto contratado que estão sob sua responsabilidade.

Fiscalização Administrativa

8.11. O Fiscal Administrativo do contrato acompanhará os aspectos administrativos contratuais quanto às obrigações previdenciárias, fiscais e trabalhistas e ao controle do contrato no que se refere a revisões, reajustes, repactuações e providências nas hipóteses de inadimplemento, segundo suas atribuições descritas no art. 24 do Decreto estadual n° 10.216, de 14 de fevereiro de 2023.

Verificação da manutenção das condições de habilitação do Fornecedor

8.12. O Fornecedor deverá manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições exigidas para a habilitação na licitação, ou para a qualificação, na contratação direta.

8.13. Constatando-se a situação de irregularidade do Fornecedor, o Gestor deverá notificar o Fornecedor para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, por motivo justo e a critério da Administração.

8.14. Não havendo regularização ou sendo a defesa considerada improcedente, a Administração deverá adotar as medidas necessárias à rescisão contratual por meio de processo administrativo, assegurado ao Fornecedor o contraditório e a ampla defesa.

8.15. Havendo a efetiva execução do objeto durante o prazo concedido para a regularização, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato.

Tópico 9 - CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

O objeto contratado sera recebido nas seguintes condições:

Recebimento do objeto

9.1 Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a Nota Fiscal ou instrumento de cobrança equivalente, pelo(a) fiscal do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os produtos ou serviços serão recebidos **definitivamente**, no prazo de 05 (cinco) dias corridos, contados do recebimento provisório, pelo Fiscal do Contrato, após a verificação da qualidade e quantidade e consequente aceitação, mediante Termo de Recebimento Definitivo, das condições exigidas no Termo de Referência.

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

9.2.2. O Recebimento provisório ou definitivo do objeto não exclui a responsabilidade do Fornecedor pelos prejuízos resultantes da incorreta execução do contrato.

9.2.3. Na hipótese de o recebimento definitivo não ser realizado no prazo fixado sem qualquer comunicação ao Fornecedor, reputar-se-á como realizada, consumando-se o recebimento no dia do esgotamento do prazo.

9.2.4. 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 federal nº 14.133, de 01 de abril 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.

9.2.5. O prazo para a solução, pelo Fornecedor, de inconsistências na execução do objeto, de saneamento da Nota Fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

9.2.6. O mero recebimento sumário de produtos pela equipe de almoxarifado, com a respectiva assinatura de canhoto da Nota Fiscal, não implicará em recebimento provisório e/ou definitivo do objeto do contrato, os quais serão formalizados por meio de documento próprio pelo respectivo fiscal do contrato.

Prazo para correção de defeitos

9.3. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação do Fornecedor, às suas custas, sem prejuízo da aplicação das penalidades.

Atesto da execução do objeto

9.4. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de atesto da execução do objeto, na forma desta seção, nos termos do art. 4º do Decreto Estadual n° 9.561 de novembro de 2019.

9.5. Havendo erro na apresentação da Nota Fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, o prazo para atesto ou liquidação ficará sobrestado até que o Fornecedor providencie as medidas saneadoras, reiniciando- se o prazo após a comprovação da regularização da situação, sem ônus à Administração.

9.6. Nenhum pagamento será efetuado ao Fornecedor enquanto perdurar pendência na apresentação da Nota Fiscal ou instrumento de cobrança equivalente.

9.7. O prazo de atesto da execução do objeto será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei Federal nº 14.133 de abril de 2021.

9.8. A Nota Fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao CADFOR.

9.8.1. O Fornecedor que estiver em situação de irregularidade junto ao CADFOR deverá entregar juntamente com a Nota Fiscal ou documento de cobrança equivalente, os documentos que porventura estiverem vencidos para fins de atualização pelo CADFOR.

9.9. A equipe de fiscalização do contrato realizará consulta ao Cadastro Unificado de Fornecedores do Estado – CADFOR, bem como no Cadastro de Inadimplentes – CADIN

estadual, para verificar a manutenção das condições de habilitação.

9.9.1. Caso seja constatado que o Fornecedor esteja em situação de irregularidade perante o Cadastro Unificado de Fornecedores do Estado – CADFOR, este será notificado por escrito para, no prazo de 5 (cinco) dias úteis, encaminhar ao Gestor do Contrato os documentos que porventura estiverem vencidos, ou, no mesmo prazo, apresentar sua defesa.

9.9.2. Caso seja constatado que o Fornecedor esteja em situação de irregularidade perante o Cadastro de Inadimplentes – CADIN estadual, este será notificado por escrito para, no prazo de 5 (cinco) dias úteis, regularizar sua situação ou, no mesmo prazo, apresentar sua defesa.

9.9.3. Os prazos referidos neste item poderão ser prorrogados uma vez, por igual período, a critério da Administração.

9.9.4. Não havendo regularização ou sendo a defesa considerada improcedente, a Administração comunicará à Controladoria-Geral do Estado a inadimplência do Fornecedor.

9.9.5. Persistindo a irregularidade, a Administração deverá adotar as medidas necessárias à rescisão dos contratos em execução, assegurado o contraditório e a ampla defesa, por meio de processo administrativo a ser instaurado.

9.9.6. Havendo a efetiva prestação dos serviços ou o fornecimento dos bens, os pagamentos serão realizados normalmente, até que se decida pela rescisão contratual, se o Fornecedor não regularizar sua situação no CADFOR e/ou no CADIN, salvo nas hipóteses em que houver indícios das infrações administrativas previstas na Lei federal nº 14.133, de 01 de abril de 2021, caso em que a retenção dos créditos não excederá o limite dos prejuízos causados à Administração.

9.10. O Gestor do Contrato deverá disponibilizar a Nota Fiscal, com seu respectivo atesto, ao setor financeiro, em até 5 (cinco) dias após o atesto.

Liquidação da Despesa

9.11. O registro da liquidação da despesa no Sistema de Programação e Execução Orçamentária e Financeira – SIOFINET deverá ser realizado pelo setor financeiro em até 15 (quinze) dias após o atesto da execução do objeto.

9.12. Para fins de liquidação, o setor financeiro deverá verificar se a Nota Fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.12.1.o prazo de validade e a data da emissão;

9.12.2. os dados do contrato e do órgão ou entidade da Administração;

9.12.3. o período respectivo de execução do contrato;

9.12.4. o valor a pagar; e

9.12.5. eventual destaque do valor de retenções tributárias cabíveis.

Prazo de Pagamento

9.13. O pagamento dos **Itens 02 e 04 de Contratação,** será realizado em 03 (três) parcelas, anuais, iguais e sucessivas, vencendo a primeira parcela em até 30 (trinta) dias corridos contados do atesto da Nota Fiscal e emissão do Termo de Recebimento Definitivo pelo Gestor do Contrato, nos termos desta seção, respeitada a ordem cronológica conforme Decreto estadual n° 9.561, de 21 de novembro de 2019, a segunda parcela 12 (doze) meses depois do adimplemento da obrigação e a terceira parcela 24 (vinte e quatro) meses depois do adimplemento da obrigação.

9.14. O pagamento referente aos **Itens 01 e 03 de Contratação** será realizado em até 30 (trinta) dias corridos após o atesto da Nota Fiscal e emissão do Termo de Recebimento Definitivo pelo Gestor do Contrato, nos termos desta seção, respeitada a ordem cronológica conforme Decreto estadual n° 9.561, de 21 de novembro de 2019.

9.15. O pagamento referente aos **Itens 05, 06 ,07 e 08 de Contratação** será realizado em até 30 (trinta) dias corridos após o atesto da Nota Fiscal e emissão do Termo de Recebimento Definitivo pelo Gestor do Contrato, nos termos desta seção, respeitada a ordem cronológica conforme Decreto estadual n° 9.561, de 21 de novembro de 2019.

9.16. A Administração somente efetuará o pagamento à proponente vencedora referente às Notas Fiscais ou documento de cobrança equivalente, estando vedada a negociação de tais títulos com terceiros.

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

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

9.17.2. Nos contratos de prestação de serviços com regime de dedicação exclusiva de mão de obra, a constatação de irregularidade no pagamento das verbas trabalhistas, previdenciárias ou relativas ao Fundo de Garantia do Tempo de Serviço – FGTS não impede o ingresso do crédito na ordem cronológica de exigibilidade, e a unidade contratante pode reter parte do montante devido ao Fornecedor, limitada a retenção ao valor do débito verificado.

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

9.18.1. A Contratante, ao efetuar o pagamento à Contratada, fica obrigada a proceder à retenção do Imposto de Renda (IR) ao Estado de Goiás com base na Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012, e alterações posteriores.

9.19. O Fornecedor regularmente optante pelo Simples Nacional, nos termos da Lei complementar nº 123, de 14 de dezembro de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Reajuste em caso de atraso no pagamento

9.20. 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 = IPCA anual acumulado (Índice de Preços ao Consumidor Ampliado do IBGE)/100.

Do reajuste do contrato

9.21 Os preços serão fixos e irreajustáveis pelo período de 12 (doze) meses contados da data do orçamento estimado. Após este período será utilizado o Índice de Custo da Tecnologia da Informação (ICTI), apurado pelo Instituto de Pesquisa Econômica Aplicada (IPEA), como índice de reajustamento.

9.22. Os reajustes a que a CONTRATADA fazer jus e não forem solicitadas durante a vigência do Contrato, serão objeto de preclusão com a assinatura da prorrogação contratual ou com o encerramento do Contrato.

Tópico 10 - FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Critério de Julgamento	Menor Preço
10.2. Forma de adjudicação	Por Lote
10.3. Participação de empresas reunidas em consórcio	não é admitida a participação de empresas reunidas em consórciom, conform item 10.21
10.4. Prazo de validade das propostas	60 dias

Tratamento diferenciado para microempresas e empresas de pequeno porte

10.5. Não será aplicado o tratamento diferenciado para microempresas (ME) e empresas de pequeno porte (EPP), previsto na Lei Complementar nº 123, de 14 de dezembro de 2006, pelas seguintes razões:

10.5.1. A presente contratação enquadra-se na hipótese de vedação do art. 4º, § 1º, inciso I, da Lei nº 14.133/2021. O valor estimado do objeto excede a receita bruta máxima admitida para o enquadramento como empresa de pequeno porte, o que afasta a aplicação dos benefícios de disputa exclusiva e de reserva de cotas.

10.5.2. Ademais, em conformidade com o Inc. II do Art. 26 da Lei Estadual Complementar nº 117/2015, o tratamento diferenciado não se mostra vantajoso para a administração pública, uma vez que o fracionamento do objeto é tecnicamente inviável e representaria grave prejuízo ao conjunto a ser contratado. A solução tecnológica não se resume a uma lista de itens independentes, mas constitui um sistema integrado e indivisível, cuja funcionalidade depende da aquisição conjunta. Os principais componentes, os appliances ADC (itens 1 e 3), são adquiridos em pares para operar em uma configuração de cluster de alta disponibilidade, atuando como uma unidade lógica única para garantir redundância e continuidade dos serviços. A divisão do fornecimento destes equipamentos entre empresas distintas impediria a formação do cluster, inviabilizando tecnicamente a arquitetura e frustrando o objetivo da contratação. Além disso, existe um vínculo indissociável entre o hardware e suas respectivas subscrições de software, garantia e suporte técnico (itens 2 e 4), que são atrelados ao número de série de cada equipamento, tornando a aquisição separada impossível. A contratação de múltiplos fornecedores para uma solução tão complexa criaria um cenário de pulverização da responsabilidade técnica, gerando um risco operacional inaceitável em caso de falhas e comprometendo a governança dos serviços. Por fim, os serviços de suporte e treinamento (itens 5 a 8) exigem um conhecimento unificado da plataforma, que somente um único responsável pode assegurar. Portanto, a contratação de uma única pessoa jurídica é medida indispensável para garantir a integridade funcional, a padronização e a performance da solução.

10.5.3. Desta forma, o certame ocorrerá por **ampla concorrência**, sendo permitida a participação de quaisquer interessados que atendam às exigências do edital, sem exclusividade ou reserva de cotas para ME e EPP.

Exigências de habilitação

10.6. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, estará definida no Edital da Licitação.

Qualificação técnica mínima exigida

10.7. A empresa deverá apresentar, no mínimo, 01 (um) atestado/declaração fornecido por pessoa jurídica de direito público ou privado, comprovando que o Fornecedor já forneceu soluções ADC da marca F5 Networks, conforme justificativa apresentada nos itens 6.4, 6.5 e 6.6, e prestou o serviço, de forma satisfatória. O atestado/declaração deverá conter, no mínimo, o nome da empresa/órgão contratante e o nome e assinatura do responsável.

10.8 A título de comprovação da qualificação técnica, o Fornecedor deve comprovar ainda:

10.8.1. Fornecimento de appliances ADC BIG-IP similares aos R10900 e/ou R5900;

10.8.2. Fornecimento de subscrições de garantia e suporte técnico do fabricante, e licenças de upgrade do software (como Best Bundle, IP Intelligence e Threat Campaigns).

10.8.3. Terá que ser comprovada a entrega e prestação do fornecimento das licenças dentro do prazo contratual, contendo informações que permitam estabelecer, por proximidade de características técnicas, comparação entre o objeto descrito no Termo de Referência e o objeto fornecido.

10.9. Diferentes atestados de objetos compatíveis fornecidos por entidades distintas poderão ser somados pelos licitantes.

10.10. Administração se resguarda no direito de diligenciar junto à pessoa jurídica emitente do Atestado ou Declaração de Capacidade Técnica, visando a obter informações sobre o serviço prestado e cópias dos respectivos contratos e aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

10.11. Não será aceito pela Administração atestado ou declaração emitido pela própria licitante, sob pena de infringência ao princípio da moralidade, pois a licitante não possui a impessoalidade necessária para atestar sua própria capacitação técnica.

Visita técnica facultativa

10.12. Considerando a natureza do objeto, não será exigida qualquer vistoria/visita técnica.

Subcontratação e participação de consórcios

10.13 Não será admitida a subcontratação do objeto.

10.13.1. O suporte técnico do fabricante da solução não caracteriza subcontratação.

10.14. A Participação de empresas reunidas em consórcio não será permitida, tendo em vista que o consórcio de empresas para fins de participação em licitação consiste na associação de empresas para um empreendimento de maior complexidade e o objeto do presente procedimento licitatório enquadra-se como objeto comum e é perfeitamente compatível para diversas empresas atuantes no ramo licitado, que apresentam o mínimo exigido no tocante à qualificação técnica e econômico-financeira, e possuem condições suficientes para a execução de contratos dessa natureza, o que não tornará restrito o universo de possíveis licitantes individuais. Ademais, a admissão de consórcio em objeto de baixa complexidade atenta contra o princípio da competitividade, pois permitiria, com o aval do Estado, a união de concorrentes que poderiam muito bem disputar entre si, violando, por via transversa, o princípio da competitividade, atingindo ainda a vantajosidade buscada pela Administração.

10.14.1. A vedação quanto à participação de consórcio, no presente procedimento licitatório, não limitará a competitividade, pois várias empresas do ramo conseguem ofertar o objeto sem a necessidade de formar consórcio;

EQUIPE DE PLANEJAMENTO RESPONSÁVEL PELA ELABORAÇÃO DESTE TERMO DE REFERÊNCIA:

Responsável	Função	Equipe
FRANCIS MARCEU DE PAIVA MENDES	Integrante Técnico	Equipe de Planejamento
BRUNO LOPES LISITA	Integrante Técnico	Equipe de Planejamento
VALDENICE NASCIMENTO DE MOURA	Integrante Administrativo	Equipe de Planejamento