PREGÃO ELETRÔNICO – PEE 2025000093

O **Serviço Nacional de Aprendizagem Comercial – Senac**, Administração Regional no Estado de São Paulo ("**Senac**"), torna pública a realização de **LICITAÇÃO**, na modalidade **PREGÃO na forma eletrônica ("Pregão"),** nos termos do **Regulamento de Licitações e Contratos do Senac – Administração Regional no Estado de São Paulo.**

RESUMO DA LICITAÇÃO

OBJETO: "ATUALIZAÇÃO TECNOLÓGICA DE BALANCEADOR E ACELERADOR DE APLICAÇÕES PARA O DATACENTER CORPORATIVO SENAC SP".

RECEBIMENTO DA PROPOSTA ELETRÔNICA NO PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO:
De 22/09/2025 até às 09h45 do dia 03/10/2025

ABERTURA DAS PROPOSTAS ELETRÔNICAS:
A partir das 10h do dia 03/10/2025.

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS:
Às 10h do dia 03/10/2025.

DISPONIBILIDADE DO EDITAL:
PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO, no site https://egov.paradigmabs.com.br/senacsp e na Sede da Administração Regional do **Senac São Paulo**, localizada na Rua Dr. Vila Nova, 228, 7º andar – Sala 705, Vila Buarque, São Paulo/SP, CEP:01222-020.

PEDIDOS E RESPOSTAS DE ESCLARECIMENTOS:
Os interessados poderão encaminhar solicitação de esclarecimentos, até o dia **29 de setembro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp , na aba "Mural", no campo "**ESCLARECIMENTOS**", em relação a eventuais dúvidas de interpretação do presente Edital e seus Anexos, visando à sua melhoria. As questões formuladas serão respondidas, por escrito, a todos os interessados, até o dia **01 de outubro de 2025**. Não serão fornecidos esclarecimentos verbais por funcionários do Senac em quaisquer fases da presente licitação.
Não serão reconhecidas dúvidas encaminhadas por outro meio que não seja o Portal de Compras e Contratações do Senac São Paulo.

Gerência de Materiais e Serviços
Senac São Paulo
Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
gms@sp.senac.br
www.sp.senac.br

PREGÃO ELETRÔNICO – PEE 2025000093

1 OBJETO

1.1 A presente licitação destina-se a "**ATUALIZAÇÃO TECNOLÓGICA DE BALANCEADOR E ACELERADOR DE APLICAÇÕES PARA O DATACENTER CORPORATIVO SENAC SP"**, conforme especificações e de acordo com as condições, quantidades e exigências descritas neste Edital.

2 CONDIÇÕES GERAIS PARA PARTICIPAÇÃO

2.1 Respeitadas as demais condições legais e as constantes deste Edital, poderão participar deste Pregão, como também firmar o contrato ou instrumento equivalente dele decorrente com o Senac, pessoas jurídicas que satisfizerem plenamente todos os termos e condições estabelecidas no Edital e seus anexos.

2.2 Na presente licitação somente poderá se manifestar em nome da Licitante o sócio ou dirigente/administrador, com poderes conferidos pelo Estatuto ou Contrato Social em vigor, procurador devidamente credenciado, ou seja, com poderes outorgados por meio de procuração, instrumento público ou particular, para representar a Licitante em processos licitatórios.

2.2.1 Somente poderão participar desta licitação as empresas **cujo ramo de atividade seja compatível com o objeto do presente Pregão**.

2.2.2 A participação na presente Licitação implica na aceitação integral e incondicional de todos os termos e condições constantes neste Edital e todos os seus anexos.

2.2.3 É vedado a qualquer pessoa física ou jurídica representar mais de uma Licitante na presente licitação.

2.3 **Não poderão participar do presente Pregão as empresas:**

a) Suspensas de licitar ou contratar com o Senac;
b) Em processo de falência, em recuperação judicial ou extrajudicial, em dissolução ou liquidação;
c) Consorciadas;
d) Que tenham em sua composição societária participação comum;
e) Que detenham um mesmo representante em comum.

2.3.1 A participação de empresas que estejam em recuperação judicial somente será permitida se amparada em certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório e desde que observadas as demais condições de habilitação.

2.4 Será **excluída sumariamente da licitação** a Licitante que estiver incursa em qualquer uma das vedações acima dispostas, **não cabendo interposição de recurso.**

2.5 A Licitante declara que leu e concorda com todos os termos do Código de Ética e Conduta Profissional do Senac São Paulo, disponível no http://sisnormas.sp.senac.br/sisnormas/downloads/codigo_de_etica_e_conduta_profissional_do_senac, e compromete-se a observá-lo e a cumpri-lo integralmente.

3 DO ACESSO AO PORTAL DE COMPRAS E CONTRATAÇÕES DO SENAC SÃO PAULO

3.1 Para participar do presente Pregão Eletrônico, os interessados deverão acessar o Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, para realizar o seu registro ou atualização cadastral, sendo, no mínimo, tipo **Básico**, com login e senha de acesso.

3.1.1 Para participação, o registro e/ou atualização cadastral, a homologação do cadastro pelo Senac, o credenciamento dos representantes que atuarão em nome da Licitante no Portal de Compras e Contratações do Senac São Paulo, bem como a senha de acesso deverá ser obtido **ANTERIORMENTE** à data de abertura da sessão pública.

3.1.2 O cadastro do interessado junto ao Sistema Eletrônico implica a responsabilidade legal pelos atos praticados e presunção de sua capacidade técnica e jurídica para realização das transações inerentes ao Pregão Eletrônico.

3.1.3 A Licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras as suas propostas e lances, sendo de sua inteira e exclusiva responsabilidade o uso da senha de acesso, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Senac, qualquer

responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

4 CONEXÃO COM O SISTEMA

4.1 Caberá à Licitante permanecer conectada ao Sistema Eletrônico para o acompanhamento das operações durante a sessão do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo Sistema Eletrônico ou de sua desconexão.

4.2 A participação neste Pregão Eletrônico se dará, exclusivamente por meio do sistema eletrônico, utilizando-se do login e senha da Licitante e subsequente encaminhamento da proposta de preços, observadas as datas e os horários limites estabelecidos neste Edital.

4.3 A desconexão do Sistema Eletrônico com o Pregoeiro, durante a sessão, implicará as seguintes questões:

4.3.1 Fora da etapa de lances, a sua suspensão e o seu reinício, desde o ponto em que a sessão foi interrompida. Neste caso, se a desconexão persistir por tempo superior a 15 (quinze) minutos, a sessão será suspensa e retomada somente após comunicação expressa às Licitantes de nova data e horário para a sua continuidade;

4.3.2 Ocorrendo a desconexão com o Pregoeiro no decorrer da etapa de lances, mas o Sistema Eletrônico permanecer acessível às Licitantes, os lances continuarão sendo recebidos sem prejuízo dos atos realizados;

4.3.3 Quando a desconexão citada no **subitem 4.3.2** persistir por tempo **superior a 10 (dez) minutos**, a sessão poderá ser suspensa e retomada somente após a comunicação expressa do Pregoeiro às Licitantes.

4.4 A desconexão do Sistema Eletrônico com qualquer Licitante não prejudicará a conclusão válida da sessão ou da licitação.

5 HABILITAÇÃO

5.1 HABILITAÇÃO JURÍDICA

5.1.1 Ato constitutivo da sociedade, em conformidade com a legislação vigente (Estatuto, Contrato Social ou outro pertinente à constituição da empresa), acompanhado de todas as suas alterações, quando houver, ou a última alteração consolidada, devidamente registradas, acompanhadas, quando aplicável, dos respectivos documentos de eleição de seus administradores;

5.1.2 Prova de registro, no órgão competente, no caso de empresário individual;

5.1.3 Ato de nomeações ou de eleição dos administradores, devidamente registrados no órgão competente, nas hipóteses de terem sido nomeados ou eleitos em separado, sem prejuízo da apresentação dos demais documentos exigidos no **Item 5.1.1**;

5.1.4 Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, bem como ato de registro ou autorização para funcionamento expedido pelo órgão competente quando a atividade assim o exigir.

5.2 REGULARIDADE FISCAL:

5.2.1 Prova de inscrição atualizada no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda – CNPJ, com situação ativa, relativa à sede da Licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

5.2.2 Prova de regularidade para com as fazendas federal, estadual e municipal do domicílio ou sede da Licitante, **na forma da lei**, por meio dos seguintes documentos:

5.2.2.1. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Federais** e Dívida Ativa da União, previstas nas alíneas "a" a "d" do parágrafo único do artigo 11 da Lei 8.212 de 24 de julho de 1991, expedida pela Secretaria da Receita Federal do Brasil ou Procuradoria Geral da Fazenda Nacional, nos termos da Portaria MF 358 de 05/09/2014;

5.2.2.2. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Estaduais** com referência especificamente ao ICMS – Imposto Sobre Circulação de Mercadorias e Serviços, expedida pela Fazenda Estadual, da sede da Licitante;

5.2.2.2.1. Em se tratando de sede no Estado de São Paulo, será aceita tanto a Certidão Negativa de Débitos Tributários da Dívida Ativa do Estado de São Paulo – CRDA, expedida pela Procuradoria Geral do Estado, quanto a Certidão Negativa de Débitos Tributários Não Inscritos na Dívida Ativa do Estado de São Paulo, expedida pela Secretaria da Fazenda do Estado de São Paulo;

5.2.2.2.2. Certidão Negativa ou Positiva com efeitos de Negativa de Débitos relativa aos **Tributos Municipais Mobiliários** com referência especificamente ao ISS – Imposto Sobre Serviços, expedida pela Secretaria da Fazenda Municipal;

5.2.3 Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço – CRF-FGTS relativo à sede da Licitante, expedida pela Caixa Econômica Federal.

5.3 QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

5.3.1 Certidão Negativa de Falência, Concordata e Recuperação Judicial e Extrajudicial, expedida pelo Distribuidor Cível da Matriz da Licitante, com validade na data de abertura da presente Licitação.

5.4 QUALIFICAÇÃO TÉCNICA

5.4.1 O pregoeiro convocará, a empresa ofertante do menor preço para entregar documento emitido pelo fabricante F5 NETWORK (no formato eletrônico) de que a Licitante é capacitada para fornecer soluções F5 NETWORKS, sendo assim apto para fornecer os produtos e serviços com excelência, a fim de não haver problemas com a garantia e o suporte técnico junto ao fabricante, sob pena de desclassificação de sua proposta.

5.4.2 CERTIFICAÇÃO TÉCNICA PARA EQUIPE OPERACIONAL

5.4.2.1 A Comissão Permanente de licitação convocará, a empresa ofertante do menor preço para entregar as certificações da equipe operacional no formato eletrônico:

5.4.2.1.1. Prova documental, mediante apresentação de certificação "Red Hat Certified System Administrator (RHCSA)", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.2.1.2. Prova documental, mediante apresentação de certificação "Securing Applications with NGINX", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.2.1.3. Prova documental, mediante apresentação de certificação "NGINX Core", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.2.1.4. Prova documental, mediante apresentação de certificação "NGINX Advanced Load Balancing", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.2.1.5. Prova documental, mediante apresentação de certificação "Configuring Caching using NGINX (Self-Directed Training)", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.2.1.6. Prova documental, mediante apresentação de certificação "Dynatrace Certified Associate", comprovando que empresa possui ao menos 1 (um) profissional certificado.

5.4.3 Os profissionais certificados devem possuir vínculo profissional com a empresa licitante e este deve ser comprovado por meio de:

5.4.3.1 Carteira de Trabalho (CTPS), comprovando o vínculo empregatício do profissional com a Licitante na data da licitação;

5.4.3.2 Contrato Social ou Estatuto, no caso de ser sócio proprietário da empresa Licitante;

5.4.3.3 Contrato de Prestação de Serviços, firmado entre o profissional com a empresa Licitante.

5.4.4.1 Todos os documentos devem ser apresentados por meio eletrônico.

5.5 CONSIDERAÇÕES GERAIS SOBRE OS DOCUMENTOS

5.5.1 Os documentos que forem emitidos pela internet estarão sujeitos a posterior conferência na página eletrônica do órgão emissor.

5.5.2 Para dirimir dúvidas suscitadas no exame dos documentos de habilitação e/ou da proposta comercial, a Comissão Permanente de Licitação, em qualquer fase da licitação, poderá, a seu critério exclusivo, realizar diligências junto às Licitantes e/ou terceiros solicitando esclarecimentos e/ou comprovação a respeito da veracidade de informações e/ou dos documentos apresentados.

5.5.3 A Comissão Permanente de Licitação poderá, ainda, a seu critério, solicitar que qualquer Licitante supra ou saneie eventuais omissões ou falhas relativas no cumprimento dos requisitos e condições estabelecidos neste Edital, mediante a apresentação de documentos desde que os envie no curso da própria sessão **no prazo previamente estipulado**.

5.5.4 Com o objetivo de dirimir dúvidas suscitadas no exame dos documentos de habilitação e/ou da proposta comercial e/ou sanear eventuais omissões ou falhas relativas no cumprimento dos requisitos e condições estabelecidos neste Edital, o Senac poderá consultar o seu Cadastro de Fornecedores.

5.5.5 Todos as certidões elencadas acima, após solicitados pelo Pregoeiro, deverão **estar válidos na data da sua apresentação**. A validade corresponderá ao prazo fixado nas próprias certidões, quando houver. Caso estas não contenham expressamente o prazo de validade, o Senac convenciona o prazo de **90 (noventa) dias corridos**, a contar da data de sua expedição, ressalvada a hipótese da Licitante comprovar que o documento tem prazo de validade inferior ou superior ao antes convencionado, mediante juntada de norma legal pertinente.

5.5.6 Independentemente de declaração expressa, a apresentação dos documentos de habilitação e da proposta ajustada implica a aceitação

plena e total das condições e exigências deste Edital e seus Anexos, a veracidade e autenticidade das informações constantes na proposta ajustada e nos documentos de habilitação apresentados, e ainda, a inexistência de fato impeditivo à participação da Licitante, o qual, na incidência, obriga a Licitante a comunicar ao Senac quando ocorrido durante o certame.

5.5.7 O desatendimento de exigências meramente formais que não comprometam a aferição da qualificação do Licitante ou a compreensão do conteúdo de sua proposta não importará seu afastamento da licitação ou a invalidação do processo.

5.5.8 É permitida a inclusão de documento complementar ou atualizado, desde que não alterem a substância das propostas, dos documentos e sua validade jurídica e seja comprobatório de condição atendida pelo Licitante quando apresentada sua proposta, que não foi juntado com os demais documentos por equívoco ou falha, o qual deverá ser solicitado e avaliado pela comissão de licitação/pregoeiro.

5.5.9 Não serão levados em consideração os documentos e/ou propostas que não estiverem de acordo com as condições deste Edital e seus Anexos, quer por omissão, quer por discordância.

6 PROCEDIMENTOS LICITATÓRIOS

6.4 INÍCIO PARA CADASTRAMENTO E RECEBIMENTO DAS PROPOSTAS ELETRÔNICAS

6.1.1 O início para cadastramento das propostas se dará a partir do dia **22 de setembro de 2025**.

6.1.2 A Licitante deverá preencher sua proposta exclusivamente no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, em conformidade com as exigências deste Edital.

6.1.3 Até às **09h45 o dia 03/10/2025**, os interessados poderão inserir ou substituir propostas de preços no sistema eletrônico. Após a abertura das propostas, não será admitido o envio/substituição de propostas comerciais.

6.1.4 Em nenhuma hipótese será admitida a identificação da Licitante, sob pena de desclassificação.

6.1.5 O valor inserido no sistema sempre será pelo **Valor Global** conforme apresentado no modelo de proposta **Anexo I**.

6.1.6 Nos preços deverão estar inclusos, além das taxas, impostos e encargos, os valores pertinentes a todas as despesas e demais custos que possam influir direta ou indiretamente na prestação dos serviços, objeto da presente licitação.

6.1.7 O valor proposto para o fornecimento será de exclusiva e total responsabilidade da Licitante, sendo considerado como justo e suficiente para a contratação oriunda da presente licitação.

6.1.8 No caso de empate entre 2 (dois) ou mais lances, o desempate se fará automaticamente pelo sistema, com base no horário do primeiro lance cadastrado.

6.1.9 **PROPOSTA AJUSTADA**: Proposta detalhada **(Anexo I**) enviada pela Licitante arrematante, apresentada em papel timbrado com identificação da Licitante, sem emendas, rasuras, assinada na última página e rubricada nas demais pelo representante legal da Licitante:

6.1.9.1 Deverá apresentar prazo de validade da proposta, valor unitário e valor total arrematado;

6.1.9.2 Deverá conter a vigência, conforme descrito no **Anexo II – Termo de Referência**;

6.1.9.3 Havendo divergência entre o preço unitário e total da proposta ajustada, prevalecerá o valor global arrematado e, havendo discordância entre o valor total da proposta em algarismo e o total por extenso, prevalecerá o que equivale ao valor arrematado.

6.1.10 A validade da proposta não poderá ser inferior a **90 (noventa) dias corridos** a contar da data de estabelecimento do valor final negociado. Não sendo indicado o prazo de validade, fica subentendido como de 90 (noventa) dias corridos.

6.1.11 Caso haja o vencimento da validade da proposta sem que a licitação tenha sido homologada e adjudicada e o contrato ou instrumento equivalente assinado, esta ficará automaticamente prorrogada, exceto se houver manifestação contrária formal da Licitante, pelo e-mail licitacao.gms@sp.senac.br, na data de vencimento da proposta, dirigida à Comissão de Licitação, caracterizando seu declínio em continuar na licitação.

6.1.12 Os termos constantes da proposta de preços da arrematante são de exclusiva responsabilidade da Licitante, não lhe assistindo o direito a qualquer modificação, após seu envio, sem a prévia concordância ou solicitação pela Comissão de Licitação.

7 ESCLARECIMENTOS DE DÚVIDAS:

7.4 Os interessados poderão encaminhar solicitação de esclarecimentos, por escrito, até às **23h59 do dia 29 de setembro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, na aba "Mural", no campo "**ESCLARECIMENTOS**".

7.5 Os esclarecimentos de dúvidas registrados no Portal de Compras e Contratações do Senac São Paulo deverão ser exclusivamente para questões relativas à presente licitação.

7.2.1 Não serão reconhecidas dúvidas encaminhadas por outro meio que não seja o Portal de Compras e Contratações do Senac São Paulo.

7.6 As questões formuladas serão respondidas, por escrito, a todos os interessados, até o dia **01 de outubro de 2025**, por meio do Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, na aba "Mural", no campo "**ESCLARECIMENTOS**". Não serão fornecidos esclarecimentos verbais por funcionários do Senac em quaisquer fases da presente licitação.

7.7 Os pedidos de esclarecimentos não suspendem os prazos previstos na licitação.

7.8 Caso a resposta ao esclarecimento resulte em modificação do presente Edital, será providenciada nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto quando a alteração não comprometer a formulação das propostas.

7.9 Os esclarecimentos formulados, bem como suas respostas, passarão a integrar o presente Edital, independentemente de sua transcrição.

7.10 Não sendo formuladas solicitações de esclarecimentos e/ou informações até a data estabelecida, ocorrerá a preclusão do direito de apresentar quaisquer questionamentos ao presente Edital, suas cláusulas e anexos.

7.11 É de responsabilidade do interessado e de cada Licitante o acompanhamento de todas as informações no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, durante todo o processo licitatório, ficando desonerado o Senac da obrigação de prestar informação' por qualquer outro meio de comunicação.

8 ABERTURA DAS PROPOSTAS ELETRÔNICAS

8.4 As **10h00 do dia 03 de outubro de 2025**, procederemos a abertura das propostas de preços no sistema eletrônico.

8.5 A apresentação da proposta eletrônica pressupõe o fiel cumprimento do estabelecido neste Edital e seus **Anexos**, inferindo-se, portanto, a não necessidade de análise para fins de classificação de propostas. Não obstante ao disposto neste subitem, o Pregoeiro, a seu exclusivo critério, poderá optar por realizar a referida análise e desclassificar as propostas que não estejam de acordo com o estabelecido neste Edital e seus Anexos, cabendo ao Pregoeiro registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real pelas Licitantes.

8.2.1 Caso o Pregoeiro opte por realizar análise de propostas, da decisão de desclassificação somente caberá pedido de reconsideração ao Pregoeiro, a ser enviado exclusivamente por meio do Sistema Eletrônico, acompanhado da justificativa de suas razões, no **prazo de 3 (três) minutos** a contar do momento em que vier a ser disponibilizada no sistema eletrônico a decisão a ser impugnada.

8.2.2 O Pregoeiro analisará e decidirá, **no mesmo prazo**, salvo motivos que justifiquem a sua prorrogação, sendo-lhe facultado, para tanto, suspender a sessão, registrar e disponibilizar a decisão no Sistema Eletrônico para acompanhamento em tempo real das Licitantes.

8.2.3 Havendo necessidade, o Pregoeiro poderá suspender a sessão, informando no "chat" a nova data e horário para continuidade.

8.2.4 **Da decisão do Pregoeiro relativa ao pedido de reconsideração não caberá recurso.**

8.2.5 Serão, ainda, desclassificadas as propostas que sejam omissas, vagas, com valores simbólicos, irrisórios, de valor zero ou que apresentem irregularidades capazes de dificultar o julgamento.

8.6 ABERTURA DA FASE DE LANCES E NEGOCIAÇÃO

8.3.1 A disputa de lances ocorrerá em modo aberto, conjuntamente, com critério de julgamento **Menor Preço Global**, e terá início às **10h00 do dia 03 de outubro de 2025**. As Licitantes classificadas poderão oferecer lances exclusivamente pelo sistema eletrônico, sem restrições de quantidades de lances ou de qualquer ordem classificatória ou cronológica específica, mas sempre inferior ao seu último lance ofertado.

8.3.2 A formulação de lances será efetuada, exclusivamente, por meio do Sistema Eletrônico e em campo específico, sendo que os valores lançados via "chat" serão desconsiderados.

8.3.3 Todos os lances oferecidos serão registrados pelo Sistema Eletrônico, que indicará o lance de menor valor para acompanhamento em tempo real pelas Licitantes.

8.3.4 O Sistema Eletrônico não identificará os autores dos lances aos demais participantes durante o transcurso da sessão.

8.3.5 A Licitante poderá ofertar novo lance, desde que inferior ao último por ela ofertado e registrado no Sistema Eletrônico.

8.3.6 Na hipótese de haver lances iguais, prevalecerá como de menor valor o lance que tiver sido primeiramente registrado.

8.3.7 A Licitante poderá oferecer lances sucessivos, observando o horário fixado e as regras de aceitação dos lances.

8.3.8 A etapa de lances terá duração de **10 (dez) minutos** e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos **últimos 2 (dois) minutos** do período de duração da sessão.

8.3.9 A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de **2 (dois) minutos** e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.3.10 Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão de disputa encerrar-se-á automaticamente.

8.3.11 Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá a Comissão Permanente de Licitação, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

8.3.12 Durante a sessão, as Licitantes serão informadas, em tempo real, sobre o valor do menor lance registrado, sem identificação da Licitante.

8.3.13 Encerrada a etapa de lances, o Sistema Eletrônico divulgará a nova grade ordenatória, contendo a classificação final, em ordem crescente de valores. Para essa classificação será considerado o último preço admitido de cada Licitante.

8.3.14 Após o encerramento da etapa de lances, o Pregoeiro poderá encaminhar, pelo Sistema Eletrônico, contraproposta à Licitante que tenha apresentado o lance mais vantajoso, para que seja obtida uma melhor proposta, observando o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital.

8.3.15 A **negociação** será realizada por meio do Sistema Eletrônico, podendo ser acompanhada pelas demais licitantes.

8.3.16 O critério de **aceitabilidade** dos preços ofertados será o de compatibilidade com os preços dos insumos e salários praticados no mercado, coerentes com a execução do objeto ora licitado, acrescidos dos respectivos encargos sociais e benefícios e despesas indiretas (BDI).

8.3.17 O Pregoeiro poderá, a qualquer momento, solicitar às Licitantes a composição de preços unitários de serviços e/ou de materiais/equipamentos, bem como os demais esclarecimentos que julgar necessário para comprovação da exequibilidade dos preços apresentados, sob pena de desclassificação.

8.3.18 Encerrada a fase de lances e após a negociação, se houver, o Pregoeiro solicitará à empresa classificada em primeiro lugar o envio da **Proposta Comercial atualizada** pelo Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, que deverá ser encaminhada no prazo por ele estabelecido, contendo o carimbo do CNPJ, nome e CPF do representante legal e sua assinatura, para análise e aprovação.

8.3.19 Caso não seja apresentada a Proposta Comercial atualizada, a Comissão Permanente de Licitação poderá convocar o segundo menor lance e, se necessário, observada a ordem crescente de preço, as Licitantes dos demais lances, desde que atendam ao critério de aceitabilidade estabelecido no Edital.

8.7 ENVIO DOS DOCUMENTOS DE HABILITAÇÃO E PROPOSTA DE PREÇOS AJUSTADA

8.4.1 Ordenados os lances em forma crescente de preço, o Pregoeiro determinará a Licitante classificada em primeiro lugar para, **em até 2 (duas) horas ou em prazo acordado dentro da própria sessão** disponibilizar **a Proposta Ajustada** conforme previsto no **subitem 6.1.9** e documentos de Habilitação descritos no **item 5 e seus subitens** deste Edital.

8.4.2 O prazo estabelecido poderá ser prorrogado por solicitação escrita e justificada do Licitante dentro do próprio sistema, formulada antes de findo o prazo, e formalmente aceita pelo pregoeiro.

8.4.3 Caso a Licitante possua o registro cadastral atualizado e as exigências atendidas, sua habilitação será reconhecida.

8.4.4 Será **inabilitada** a Licitante que deixar de apresentar ou apresentar em desacordo qualquer um dos documentos exigidos no item 5 deste Edital, ou, quando for o caso, estar com seu respectivo **registro cadastral desatualizado e não atualizá-lo no prazo concedido pela Comissão Permanente de Licitação**.

8.4.4.1 Na hipótese de inabilitação, caberá à Comissão Permanente de Licitação autorizar o Pregoeiro a convocar a Licitante do segundo menor lance e, se necessário, observada a ordem

crescente de preço, as Licitantes dos demais lances, desde que atendam ao critério de aceitabilidade estabelecido neste Edital.

8.4.4.2 O Pregoeiro poderá adotar os mesmos critérios de negociação descritos no item 8.

8.4.5 Na hipótese de inabilitação de todos os Licitantes ou de desclassificação de todas as propostas, a Comissão Permanente de Licitação poderá, a seu exclusivo critério, fixar prazo comum a todas as Licitantes para retificações, livres das causas que deram origem à inabilitação ou à desclassificação.

8.8 DA HABILITAÇÃO COM REGISTRO CADASTRAL

8.5.1 A Licitante que estiver com o registro cadastral **atualizado** no Cadastro de Fornecedores do Senac São Paulo poderá ser dispensada da apresentação dos **documentos de habilitação jurídica e regularidade fiscal**, ficando obrigatória a apresentação dos demais documentos exigidos no item 5.

8.5.2 A Licitante que estiver com o registro cadastral desatualizado poderá proceder à respectiva atualização acessando o Cadastro de Fornecedores no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, até a **data de abertura**.

8.5.3 Quaisquer informações ou dúvidas inerentes ao registro cadastral deverão ser encaminhadas nos termos do subitem 7.1.

8.5.4 Caso a Licitante não utilize as hipóteses do registro cadastral, deverá cumprir todas as exigências previstas no **item 5** (Documentos de Habilitação).

9 DECLARAÇÃO DA LICITANTE VENCEDORA

9.4 Realizada a análise da proposta ajustada e dos documentos de habilitação, o Pregoeiro indicará a Licitante vencedora e o processo será encaminhado à autoridade competente para homologação e adjudicação.

10 DOS RECURSOS

10.4 Divulgada a(s) vencedora(s) por decisão da Comissão Permanente de Licitação, a Licitante que dela discordar terá o prazo de **até 5 (cinco)**

minutos para manifestar sua intenção de interpor recurso, em campo próprio do Sistema Eletrônico. A partir da aceitabilidade do recurso, a Licitante terá o prazo de **2 (dois) dias úteis** para apresentação das razões da interposição do recurso também no Sistema Eletrônico.

10.5 Interposto o recurso nos termos do subitem 10.1, dele se dará ciência às demais licitantes pelo Sistema Eletrônico, que poderão no mesmo prazo de até 2 (dois) dias úteis, para apresentar suas contrarrazões no Sistema Eletrônico. O recurso terá efeito suspensivo.

10.6 A falta de manifestação imediata e motivada da Licitante, bem como a não apresentação de documentos comprobatórios que instruam o recurso no prazo previsto no subitem 10.1, implicará a renúncia do direito de recorrer.

10.7 Na contagem dos prazos estabelecidos nos subitens 10.1 e 10.2, excluir-se-á o dia de início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos aqui referidos, em dia de funcionamento da Sede da Administração Regional do Senac São Paulo, localizada na Rua Dr. Vila Nova, 228, 7º andar, bairro Vila Buarque, São Paulo/SP.

10.8 O recurso interposto em desacordo com as condições estabelecidas neste Edital não será conhecido.

10.9 O acolhimento do recurso pela autoridade competente somente invalidará os atos insuscetíveis de aproveitamento.

11 SANÇÕES APLICÁVEIS NO PROCEDIMENTO LICITATÓRIO

11.4 A Licitante vencedora que, injustificadamente, recusar-se a assinar o contrato ou o instrumento equivalente, em prazo estipulado pela Comissão Permanente de Licitação, sujeitar-se-á aplicação das sanções de perda do direito à contratação, perda da caução em dinheiro ou execução das demais garantias de propostas oferecidas e de suspensão do direito de licitar e contratar com o Senac, pelo período de até **3 (três) anos.**

11.5 A Licitante perderá o direito de licitar com o Senac nas seguintes hipóteses:

a) Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato ou instrumento equivalente.

b) Fraudar a licitação ou praticar ato fraudulento na execução do contrato ou instrumento equivalente.

c) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.

d) Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.

e) Praticar ato lesivo previsto no artigo 5° da Lei n 12.846, de 1. ° de agosto de 2013.

11.6 Antes da aplicação de qualquer penalidade será facultada à parte contrária a defesa, mediante envio de notificação escrita à Licitante vencedora, a qual deverá ser respondida no prazo de até **5 (cinco) dias úteis** ou outro a ser fixado pelo Senac.

11.7 O descumprimento total ou parcial das condições, prazos e obrigações contratuais, relacionadas à execução do objeto, poderá ensejar a aplicação das sanções previstas no contrato ou instrumento equivalente, sem prejuízo da responsabilização civil e penal, garantindo-se em qualquer hipótese o direito ao contraditório e à ampla defesa.

12 PROTEÇÃO DE DADOS PESSOAIS

12.4 O Senac tem compromisso com a privacidade e a proteção de dados pessoais de seus alunos, colaboradores, fornecedores, clientes e parceiros. E, nesse sentido, o Senac envida seus melhores esforços para, no tratamento de dados pessoais decorrente deste Edital, observar integralmente a legislação aplicável, em especial a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais ("LGPD"), comprometendo-se, na qualidade de controlador, a:

a) Cumprir as obrigações estabelecidas pela LGPD, tratando sempre o mínimo de dados pessoais necessários para atingir as finalidades deste Edital;

b) Adotar medidas razoáveis para informar empregados e terceiros sobre cuidados e responsabilidades resultantes de normas de proteção de dados pessoais;

c) Envidar esforços razoáveis para garantir que os dados pessoais tratados estejam atualizados e sejam relevantes em todas as circunstâncias, enquanto estiverem sob sua custódia ou sob seu controle, na medida em que tenha capacidade de fazê-lo;

d) Notificar o titular de dados pessoais e as autoridades acerca do tratamento não autorizado ou ilegal, perda, destruição, dano, alteração ou divulgação não autorizada, bem como qualquer violação de medidas de segurança em relação a dados pessoais cujo tratamento decorra deste Edital; e

e) Disponibilizar avisos de privacidade para ampliar a transparência e confiabilidade acerca do tratamento de dados pessoais realizado.

12.5 Ao participar do processo licitatório objeto deste Edital, a Licitante, por seus representantes legais e sob as penas da lei, declara como verdadeiros quaisquer dados pessoais informados na Documentação de Habilitação e/ou decorrentes do previsto neste Edital, responsabilizando-se por esta garantia e pela legalidade do compartilhamento dos dados pessoais com o Senac nos termos da legislação aplicável, em particular da LGPD. A Licitante, compromete-se, ainda, a não comunicar, revelar, disponibilizar ou utilizar dados pessoais aos quais tiver acesso em razão de sua participação no processo licitatório para finalidades distintas daquelas que motivaram o seu acesso, responsabilizando-se integral e exclusivamente pelo pleno atendimento desta obrigação.

12.6 A Licitante declara, por seus representantes legais e sob as penas da lei, que conhece e cumpre integralmente as disposições da LGPD no que toca o tratamento de dados pessoais necessário para a condução de seu negócio e execução do contrato objeto desta Licitação, particularmente que (i) observa as obrigações estabelecidas pela LGPD, garantindo, inclusive, a origem lícita e/ou necessidade dos dados pessoais tratados; (ii) adota medidas razoáveis para informar empregados e terceiros sobre cuidados e responsabilidades resultantes de normas de proteção de dados pessoais; (iii) possui procedimento que permite notificar o Senac acerca do tratamento não autorizado ou ilegal, perda, destruição, dano, alteração ou divulgação não autorizada, bem como qualquer violação de medidas de segurança em relação a dados pessoais cujo tratamento decorra deste Edital e futuro contrato; e (iv) implementou mecanismos para cumprimento de solicitações envolvendo tratamento de dados pessoais pelos titulares e autoridades, e mitigação de riscos, podendo, inclusive, cooperar com o Senac nesse sentido.

12.7 A Licitante reconhece que, nos termos da legislação aplicável e políticas de privacidade e segurança da informação do Senac, bem como em decorrência deste Edital, dados pessoais serão tratados, de forma segura e em ambiente com acesso restrito, para fins especialmente de viabilizar (i) a participação na

Licitação, (ii) a contratação, a condução e gestão das atividades relacionadas ao objeto da Licitação; e (iii) o contato do Senac por qualquer meio, inclusive para participação em processos licitatórios no futuro. Declara, ainda, ciência de que os dados pessoais podem ser, nos termos da lei, compartilhados pelo Senac com outras entidades como auditores, prestadores de serviços de controle de acesso às dependências do Senac, órgãos do governo, e/ou outros terceiros, inclusive para fins de transparência, evidência da lisura do processo licitatório e atendimento a dispositivos da Lei de Acesso à Informação, sobretudo para cumprimento de obrigações legais do Senac, execução do contrato, exercício regular de direitos e atingimento de interesses legítimos.

12.8 Em caso de dúvidas acerca do tratamento de dados pessoais e/ou para exercer os direitos previstos na LGPD, como de acesso, retificação e exclusão, o titular de dados pessoais e/ou seu representante poderão entrar em contato com o encarregado de proteção de dados do Senac São Paulo em https://www.sp.senac.br/fale-com-a-gente/privacidade-de-dados.

13 DA LEI ANTICORRUPÇÃO

13.4 A Licitante deverá atender às disposições contidas na Lei nº 12.846/2013 – Lei Anticorrupção, motivo pelo qual durante todo o período de vigência da contratação, conduzirá suas práticas comerciais de forma ética e em conformidade com os preceitos legais aplicáveis, não podendo dar, oferecer, pagar, prometer pagar ou autorizar o pagamento, direta e indiretamente, de qualquer valor, a quem quer que seja, com a finalidade de influenciar qualquer ato ou decisão, ou para assegurar qualquer vantagem indevida, ou direcionar negócios, e que violem o estabelecido na Lei Anticorrupção.

14 DISPOSIÇÕES GERAIS

14.4 Todas as informações da presente licitação, tais como esclarecimentos de dúvidas, erratas, julgamentos, recursos, resultados e homologação, dentre outras, serão comunicadas pelo site www.sp.senac.br/sites/licitacao. Sendo de responsabilidade de cada Licitante o devido acompanhamento e os atos praticados.

14.5 Todas as referências a horário neste Edital consideram o horário de Brasília-DF.

14.6 Caso as Licitantes declaradas vencedoras da licitação optem em fornecer os materiais/equipamentos ou prestar os serviços objeto da presente licitação por meio de estabelecimento filial, deverão realizar o cadastro ou atualização

respectiva no Cadastro de Fornecedores no Portal de Compras e Contratações do Senac São Paulo: https://egov.paradigmabs.com.br/senacsp, apresentando os documentos atualizados elencados no subitem 5 em relação à filial eleita, bem como, documentos de qualificação técnica, quando houver, exceto aqueles que pela própria natureza ou por determinação legal, forem comprovadamente emitidos apenas em favor do estabelecimento matriz ou cuja validade abranja todos os estabelecimentos da empresa, no prazo de até 2 (dois) dias úteis a contar da data de solicitação do Senac.

14.7 Se as Licitantes vencedoras não apresentarem a documentação exigida no subitem anterior, o faturamento deverá ser realizado por meio de sua sede.

14.8 As Licitantes vencedoras deverão manter as condições que propiciaram a sua habilitação e qualificação, facultando-se ao Senac, a seu exclusivo critério, realizar diligência no endereço apresentado pelas vencedoras, para comprovação de todas as exigências descritas no Edital, bem como exigir a renovação cadastral, no ato da assinatura do contrato ou instrumento equivalente, no todo ou em parte, dos documentos de habilitação e qualificação.

14.9 A definição da marca **F5 NetWorks**, está amparada em situação prevista na Resolução 18/2024, ou seja, "Na definição do objeto e para atendimento das necessidades da contratante, poderá ser realizada a indicação de características e especificações exclusivas ou marcas mediante justificativa técnica.

14.10 O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que seja possível a aferição da sua qualificação ou a exata compreensão da sua proposta.

14.11 O Senac poderá exigir a prestação de garantia contratual e, conforme o caso, de garantia adicional, nos termos que vierem a ser estabelecidos no contrato ou instrumento equivalente.

14.12 A Comissão de Licitação tem o direito de exigir, a qualquer época ou oportunidade, documentos ou informações complementares que julgar necessários ao entendimento e comprovação dos documentos apresentados.

14.13 A Comissão de Licitação poderá efetuar visita às instalações da Licitante classificada em primeiro lugar para confirmar as reais condições para atendimento do objeto desta licitação. Caso seja verificada a incapacidade do

atendimento, a Licitante poderá ser desclassificada, a critério da Comissão de Licitação.

14.14 A Comissão de Licitação poderá, no interesse do Senac em manter o caráter competitivo desta licitação, relevar omissões puramente formais nos documentos e propostas apresentadas pela Licitante. Poderá, também, realizar pesquisa na internet, quando possível para verificar a regularidade/validade de documentos ou fixar prazo às Licitantes para dirimir eventuais dúvidas. O resultado de tais procedimentos será determinante para fins de habilitação.

14.15 Não serão levados em consideração os documentos e proposta que não estiverem de acordo com as condições deste Edital e seus Anexos, quer por omissão, quer por discordância.

14.16 Admitir-se-á a continuidade do contrato ou instrumento equivalente celebrado com a Licitante vencedora que tenha sofrido operações de reorganização societária, tais como cessão ou transferência total ou parcial, transformação, fusão, cisão e incorporação, desde que sejam observados pela nova empresa os requisitos de habilitação previstos neste instrumento convocatório e em conformidade com o **Regulamento de Licitações e Contratos do Senac São Paulo**, e ainda, que sejam mantidas as condições inicialmente estabelecidas.

14.17 Considerando que os procedimentos licitatórios não têm natureza jurídica de propostas de contratação, o Senac São Paulo reserva o direito de adiar, cancelar, revogar, anular ou tornar sem efeito, no todo ou em parte, a presente licitação sem que isto gere aos Licitantes qualquer direito, inclusive de reparação a eventuais perdas e danos ou de lucros cessantes.

14.18 A inobservância ao Regulamento de Licitações e Contratos do Senac São Paulo pode ensejar, em caso de comprovado prejuízo ao patrimônio do Senac, a anulação da contratação resultante do procedimento irregular e a adoção de providências para responsabilização civil e penal dos que tenham contribuído com ação ou omissão para o resultado danoso.

14.19 Os prepostos da Licitante vencedora não terão vínculos empregatícios e previdenciários de qualquer natureza com o Senac.

14.20 A Licitante vencedora e seus sucessores se responsabilizarão por todos e quaisquer danos e/ou prejuízos que, a qualquer título, venham causar à

imagem do Senac e/ou terceiros, em decorrência da execução indevida do objeto desta licitação.

14.21 A Licitante declara ter ciência e se compromete a cumprir os princípios e regras contidos no Código de Ética do Senac São Paulo, disposto no site: http://sisnormas.sp.senac.br/sisnormas/downloads/codigo_de_etica_e_conduta_profissional_do_senac.

14.22 Considerando as medidas de segurança e boas práticas adotadas pelo Senac São Paulo, será de responsabilidade da Licitante a confirmação do recebimento dos e-mails enviados para o endereço eletrônico licitacao.gms@sp.senac.br. O Senac não se responsabilizará por e-mails não recebidos e não confirmados pela Licitante, independente do motivo que o ensejou.

14.23 Fica eleito o Foro da Comarca da Capital do Estado de São Paulo, para dirimir quaisquer dúvidas referentes ao presente Edital.

14.24 Fazem parte integrante deste Edital, os seguintes Anexos:

Anexo I – Modelo de Proposta
Anexo II – Termo de Referência

São Paulo, 22 de setembro de 2025.

Serviço Nacional de Aprendizagem Comercial – Senac
Administração Regional no Estado de São Paulo
Gerência de Materiais e Serviços

ANEXO I
MODELO DE PROPOSTA COMERCIAL
PREGÃO ELETRÔNICO - PEE 2025000093

(M O D E L O) - (Emitir em papel timbrado da Licitante)

	Item	Descrição	QTD	Valor Unitário	Valor Total
LOTE	1	Solução de balanceamento e proteção de avançada de aplicações WEB via appliance físico garantia 12 meses	2	R$	R$
	2	Serviço de Licenciamento e Garantia da Solução Implantada	1	R$	R$
	3	Serviço de Suporte 12 Meses	1	R$	R$
	4	Treinamento	1	R$	R$
	VALOR TOTAL			R$	

** Preços com duas casas decimais.*
*** Os valores informados deverão estar com todos os impostos inclusos.*

Obs.:
1) Validade da Proposta: 90 (noventa) dias;
2) Condições de Pagamento: 30 (Trinta) dias;
3) Prazo de Entrega: 120 dias;
4) Vigência dos Serviços: 12 Meses
5) Local de Entrega: Rua Doutor Vila Nova, número 228 - 10º andar
6) Dados da empresa que efetuará o faturamento:
Razão Social:.....
Endereço:.....Cep.....Bairro.....Município.....Estado.....
CNPJ .....
Inscrição Estadual .....
Contato.....Fone.....Fax.....
E-Mail .....

Localidade, dia, mês e ano.

Assinatura
(nome completo e cargo do representante legal da Empresa – somente sócios administradores / proprietários ou procuradores com poderes específicos).

Gerência de Materiais e Serviços
Senac São Paulo
Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
gms@sp.senac.br
www.sp.senac.br

ANEXO II
TERMO DE REFERÊNCIA
PREGÃO ELETRÔNICO Nº PEE 2025000093

1. OBJETIVO

1.1. Atualização tecnológica de Balanceador e Acelerador de Aplicações para o Datacenter Corporativo Senac SP.

2. JUSTIFICATIVA

2.1. Este produto está relacionado ao projeto de alta disponibilidade para as principais aplicações e servidores publicados na internet do Senac SP, além de atender as novas demandas relacionadas a recursos de acessos externos originados da internet e ampliar nossos serviços, proporcionando contingenciamento, balanceamento, aceleração e maior números de conexões simultâneas sem afetar a performance das aplicações ou servidores.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Especificação Técnica – Quantidade: 2 Unidades

Os appliances devem apresentar hardware para alto desempenho além de gerenciamento avançado das conexões para retirar as tarefas de processamento intensivo dos servidores de aplicações e possibilitar que esses recursos sejam utilizados de modo mais eficiente.
Os appliances devem acrescentar uma camada de segurança, fornecendo mecanismo de filtragem capaz de limitar o acesso de modo bastante granular.
O objeto desta contratação constitui-se no "refresh tecnológico" dos appliances existentes mediante a aquisição, instalação, configuração e suporte de 02 (dois) Balanceador e Acelerador de Aplicações F5 Big-IP e respectivos módulos de gerenciamento e softwares necessários, podendo ser fornecido interno ao chassi dos equipamentos ou em equipamento externo.
A solução deve garantir redundância e alta disponibilidade, provendo toda infraestrutura de hardware e/ou software suficientes e necessários ao seu completo funcionamento.
A solução deverá adaptar-se à estrutura tecnológica atualmente em funcionamento, sem necessidade de alterar a configuração do serviço de acesso aos servidores, sendo permitidos pequenos ajustes, se necessário.

Gerência de Materiais e Serviços
Senac São Paulo
Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
gms@sp.senac.br
www.sp.senac.br

Item 1 - Modelo de referência F5 Big-IP R4800 igual ou superior – Quantidade: 2 unidades

3.1.1. Todas as especificações técnicas a seguir, no entanto, descrevem as características de 1 (um) equipamento que deverá compor o cluster solicitado.

3.1.2. O equipamento deverá ser novo, de primeiro uso e acondicionado adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte;

3.1.3. Todos os equipamentos (hardwares da solução) deverão possuir as certificações expressamente impostas pela lei, tais como as certificações da ANATEL. O certificado da ANATEL deverá ser emitido para os equipamentos em nome do Fabricante da solução;

3.1.4. Não será permitido hardware de uso genérico, OEM, White Box ou do tipo PC;

3.1.5. Não será aceito soluções open-source nos componentes da solução de WAF;

3.1.6. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us do referido rack;

3.1.7. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação do equipamento no rack;

3.1.8. Possui fontes AC redundantes com tensão de entrada 90-240VAC, bi-volt automática, sendo que o equipamento continua totalmente operacional no caso de falha de uma das fontes

3.1.9. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance NGFW; possuir painel/led indicativo de on/off do uso de disco e interfaces de rede;

3.1.10. Possuir no mínimo 4 (quatro) interfaces de rede de 10GE com conectores padrão SFP+ (SR) Fiber Connector (10G-LC/850nm) ROHS;

3.1.11. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;

3.1.12. Possuir capacidade de operar, no mínimo, 40.000 (quarenta mil) transações por segundo TPS de tráfego SSL com chaves de 2048 bits;

3.1.13. Possuir capacidade de operar, no mínimo, 1.800.000 (um milhão e oitocentas mil) requisições por segundo (RPS) na camada 7;

3.1.14. Possuir capacidade de operar, no mínimo, 700.000 (setecentas mil) conexões por segundo (CPS) na camada 4;

3.1.15. Possuir capacidade de operar, no mínimo, 35.000.000 (trinta e cinco milhões) de conexões concorrentes;

3.1.16. Possuir capacidade de operar, no mínimo, 20 Gbps de tráfego SSL;

3.1.17. Possuir capacidade de processar 45 Gbps de throughput em camada 7;

3.1.18. Possuir capacidade de comprimir, no mínimo, 30 Gbps do tráfego;

3.1.19. Possuir memória RAM mínima de 64 GB;

3.1.20. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise de no mínimo 480 GB;

3.2. Requisitos gerais

3.2.1. Suportar IPv4 e IPv6;

3.2.2. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;

3.2.3. Suportar VXLAN para integração com o ambiente de virtualização;

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

3.2.5. Suportar implementação em alta disponibilidade,:

3.2.5.1. Implementar modo ativo/standby;

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

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

3.2.5.4. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, hearbeat e sincronização entre os appliances;

3.2.5.5. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

3.2.6. Permitir expansão do cluster adicionando novos appliances inclusive de modelos diferentes;

3.2.7. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;

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

3.2.9. Permitir habilitar e desabilitar acesso administrativo via SSH;

3.2.10. Manter internamente múltiplos arquivos de configurações do sistema;

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

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

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

3.2.14. 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;

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

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

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

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

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

3.2.20. Suportar a rollback de configuração e imagem;

3.2.21. 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;

3.2.22. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;

3.2.23. Permitir reiniciar o appliance pela interface gráfica e por CLI;

3.2.24. Implementar SNMPv1, SNMPv2c e SNMPV3;

3.2.25. Implementar traps SNMP;

3.2.26. Permitir a criação de MIBs customizadas;

3.2.27. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

3.2.28. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:

3.2.28.1. Coleta de métricas de desempenho compatível com Prometheus;

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

3.2.28.3. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;

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

3.2.28.5. Deve incluir métricas de requisições, respostas;

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

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

3.2.28.8. 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;

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

3.2.29. Implementar debugging utilizando CLI via console e SSH;

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

3.2.31. 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;

3.2.32. 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;

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

3.2.34. 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;

3.2.35. 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;

3.2.36. Implementar roteamento IPv4 e IPv6 estático e dinâmico;

3.2.36.1. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;

3.2.36.2. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

3.2.36.3. Suportar integração via BGP para divulgação de prefixos;

3.2.36.4. 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 appliance. 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;

3.2.36.5. Suportar Equal Cost Multipath (ECMP);

3.2.36.6. Implementar Bidirectional Forward Detection (BFD);

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

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

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

3.2.37.3. 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;

3.2.37.4. Implementar criptografia de cookies;

3.2.37.5. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;

3.2.37.6. 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;

3.2.37.7. 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;

3.2.37.8. 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;

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

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

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

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

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

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

3.2.37.15. Implementar proteção contra SYN floods;

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

3.2.37.17. 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;

3.2.37.18. Suportar Stream Control Transmission Protocol (SCTP);

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

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

3.2.37.19.2. Permitir espelhamento de tráfego de conexões TLS;

3.2.37.19.3. 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;

3.2.37.20. Em relação ao tráfego TLS, deve suportar:

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

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

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

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

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

3.2.37.21. Suportar os algoritmos para sessões TLS:

3.2.37.21.1. SSL session cache Timeout;

3.2.37.21.2. Session Ticket;

3.2.37.21.3. OCSP (Online Certificate Status Protocol) Stapling;

3.2.37.21.4. Dynamic Record Sizing;

3.2.37.21.5. ALPN (Application Layer Protocol Negotiation;

3.2.37.21.6. Perfect Forward Secrecy;

3.2.37.22. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);

3.2.37.23. Suportar importação de certificados digitais e chaves privadas;

3.2.37.24. Possuir alertas visuais na interface web de certificados com vencimento próximo;

3.2.37.25. Implementar limpeza de cabeçalho HTTP;

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

3.2.37.27. 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;

3.2.37.28. 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;

3.2.37.29. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;

3.2.37.30. 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;

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

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

3.2.37.33. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração;

3.2.37.33.1. Suportar, pelo menos, as plataformas Kubernetes "Vanilla", Red Hat OpenShift e VMware Tanzu;

3.2.37.33.2. Permitir a configuração através de ConfigMaps;

3.2.37.33.3. Permitir a configuração através de CustomResourceDefinition (CRD) da solução;

3.2.37.33.4. Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;

3.2.37.33.5. Permitir a configuração através de objetos Ingress na plataforma;

3.2.37.33.6. Permitir a configuração através de objetos Route no OpenShift;

3.2.37.33.7. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;

3.2.37.33.8. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada;

3.2.37.34. Suportar o protocolo FTP com, pelo menos, as seguintes características:

3.2.37.34.1. Determinar os comandos FTP permitidos;

3.2.37.34.2. Requests FTP anônimos;

3.2.37.34.3. Validar conformidade com o protocolo FTP;

3.2.37.34.4. Proteger contra ataques de força bruta nos logins;

3.2.37.35. Suportar o protocolo SMTP com, pelo menos, as seguintes características:

3.2.37.35.1. Limitar o número de mensagens;

3.2.37.35.2. Validar registro SPF do DNS;

3.2.37.35.3. Determinar quais métodos SMTP podem ser utilizados.

3.2.38. Implementar proteção de aplicações no nível de rede e protocolo;

3.2.38.1. 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;

3.2.38.2. Proteger de ataques DDoS nas camadas de rede e de sessão;

3.2.38.3. Proteger de ataques DDoS que utilizem SSL;

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

3.2.38.4.1. Endereço IP de destino

3.2.38.4.2. Endereço IP de origem

3.2.38.4.3. Porta de destino

3.2.38.4.4. Porta de origem

3.2.38.4.5. VLAN

3.2.38.4.6. Protocolo

3.2.38.4.7. Ação

3.2.38.4.8. Horário

3.2.38.4.9. Log;

3.2.38.4.10. Permitir definir agendamento para ativação da regra;

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

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

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

3.2.38.6.1. Permitir: os pacotes são aceitos e passam pela solução;

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

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

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

3.2.38.7.1. Global, regras válidas para todo o tráfego, independente da interface de ingresso;

3.2.38.7.2. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;

3.2.38.7.3. Objeto, regras válidas para objetos específicos;

3.2.38.8. Deve possuir criptografia IPSEC para comunicação entre sites;

3.2.38.9. 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;

3.2.38.10. Permitir a restauração das configurações de proteções originais;

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

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

3.2.38.13. 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;

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

3.2.38.15. Permitir a criação de regras de filtragem através de API REST declarativa;

3.2.38.16. A documentação da API deve ser pública;

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

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

3.2.38.19. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, BadIGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP

Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;

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

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

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

3.2.38.23. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;

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

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

3.2.38.26. Deve possuir a funcionalidade de limiares automático para vetores de DoS:

3.2.38.27. Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.

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

3.2.38.29. 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;

3.2.39. Implementar serviços de entrega de aplicações distribuídas através do serviço de DNS;

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

3.2.39.2. Implementar DNSSec, independente da estrutura dos servidores DNS em uso;

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

3.2.39.4. 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;

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

3.2.39.6. Implementar proteções contra-ataques DNS, incluindo no mínimo a inspeção de protocolo, validação de protocolo, UDP flood, pacotes malformados, teardrop e DNS Water-torture;

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

3.2.39.8. Implementar filtragem de pacotes e tipos de requisições;

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

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

3.2.39.11. Possuir base de geolocalização IP e permitir sua atualização;

3.2.39.12. Implementar DNS64 e implementar as seguintes integrações:

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

3.2.39.14. Cliente envia consulta AAAA, a solução encaminha a consulta (recursivo) com A, caso não tenha resposta, faz a consulta com AAAA, responde para o cliente um prefixo + A e AAAA

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

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

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

3.2.39.18. Suportar DNS over HTTPS (DoH);

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

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

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

3.2.39.22. Suportar IP Anycast;

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

3.2.39.24. 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;

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

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

3.2.39.27. Suportar monitores utilizando HTTPS, incluindo a validação do SNI;

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

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

3.2.39.30. 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;

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

3.2.39.32. Permitir que a contingência seja automática;

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

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

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

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

3.2.39.37. Suportar Response Policy Zones (RPZ), mecanismo de proteção de resolução para DNS recursivo que permite o tratamento customizado da resolução de nomes, capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas;

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

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

3.2.39.40. Suportar inserir o ECS para outros servidores DNS;

3.2.39.41. 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;

3.2.39.42. 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;

3.2.39.43. 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.

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

3.2.39.45. Permitir configurar rate limit realizadas via TCP ou UDP por FQND;

3.2.39.46. Permitir configurar rate limit para consultas realizadas via TCP ou UDP por IP de origem;

3.2.40. Implementar proteção para aplicações web e API contra ameaças na camada de aplicação;

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

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

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

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

3.2.40.5. Implementar modelo positivo de segurança de aplicações web;

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

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

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

3.2.40.9. 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;

3.2.40.10. Permitir desativar a inspeção para URL específicas;

3.2.40.11. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;

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

3.2.40.13. Suportar aplicações que utilizam protocolo WebSocket;

3.2.40.14. 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;

3.2.40.15. Implementar proteção contra:

3.2.40.15.1. Acesso por força bruta;

3.2.40.15.2. DoS e DDoS em camada 7;

3.2.40.15.3. Buffer Overflow;

3.2.40.15.4. Cross Site Request Forgery (CSRF);

3.2.40.15.5. Cross-Site Scripting (XSS);

3.2.40.15.6. Server-Side Request Forgery (SSRF);

3.2.40.15.7. SQL Injection;

3.2.40.15.8. Parameter tampering;

3.2.40.15.9. Cookie poisoning;

3.2.40.15.10. HTTP Request Smuggling;

3.2.40.15.11. Manipulação de campos escondidos (hidden input);

3.2.40.15.12. Manipulação de cookies;

3.2.40.15.13. Roubo de sessão através de manipulação de cookies;

3.2.40.15.14. Sequestro de sessão;

3.2.40.15.15. Validação de consistência de formulários;

3.2.40.15.16. Validação do cabeçalho do "user-agent" para identificar clientes inválidos;

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

3.2.40.17. Suportar codificação HTML "application/x-www-form-urlencoded";

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

3.2.40.19. Suportar codificação fragmentada (chunked encoding);

3.2.40.20. Suportar validações de protocolo:

3.2.40.20.1. Restrição de métodos;

3.2.40.20.2. Restrição de protocolos e versões;

3.2.40.20.3. Validação de conformidade com RFCs;

3.2.40.20.4. Validação de caracteres URL-encoded;

3.2.40.20.5. Validação de codificação fora de padrão %uXXYY.

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

3.2.40.22. Possuir técnicas de detecção de evasões:

3.2.40.22.1. URL-decoding;

3.2.40.22.2. Terminação Null Byte String;

3.2.40.22.3. Paths autorreferenciados;

3.2.40.22.4. Case de caracteres misturados;

3.2.40.22.5. Uso excessivo de espaços em branco;

3.2.40.22.6. Decodificação de entidades HTML;

3.2.40.22.7. Caracteres de escape;

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

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

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

3.2.40.26. Implementar validação de URL;

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

3.2.40.28. 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;

3.2.40.29. Suportar aplicações Single-Page Application (SPA);

3.2.40.30. Permitir a customização da resposta de bloqueio;

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

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

3.2.40.33. Implementar as proteções:

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

3.2.40.33.2. Ocultar qualquer mensagem de erro HTTP dos usuários;

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

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

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

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

3.2.40.37. Implementar aprendizado automático de XML;

3.2.40.38. Permitir a importação de arquivo de esquema XML;

3.2.40.39. Implementar aprendizado automático de JSON;

3.2.40.40. Permitir a importação de arquivo de esquema JSON;

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

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

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

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

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

3.2.40.46. 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;

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

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

3.2.40.49. 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;

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

3.2.40.51. Possuir proteções contra XML Bomb;

3.2.40.52. 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;

3.2.40.53. 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;

3.2.40.54. 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;

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

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

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

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

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

3.2.40.54.6. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;

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

3.2.40.55. 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;

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

3.2.40.57. 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;

3.2.40.57.1. Identificar ataques com diferentes usuários e mesma origem;

3.2.40.57.2. Identificar ataques com diferentes origens e mesmo usuário;

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

3.2.40.58. 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;

3.2.40.59. 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;

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

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

3.2.40.61. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.

3.2.40.62. Possuir atualização automática de definição de bots;

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

3.2.40.64. Permitir a criação de definições de bots;

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

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

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

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

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

3.2.40.70. 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;

3.2.40.71. 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;

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

3.2.40.73. 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;

3.2.40.74. 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;

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

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

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

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

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

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

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

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

3.2.40.83. 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);

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

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

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

3.2.40.87. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de

forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;

3.2.41. Suportar integração com funcionalidade de gestão avançada de tráfego automatizado do mesmo fabricante para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador;

3.2.42. Implementar bases de inteligência de ameaças atualizadas automaticamente.

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

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

3.2.42.3. 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;

3.2.42.3.1. 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;

3.2.42.3.2. 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;

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

3.2.42.3.4. 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;

3.2.43. Implementar painéis para monitoramento da solução;

3.2.43.1. 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;

3.2.43.2. Possuir relatórios de proteção do serviço de DNS, incluindo eventos por período, eventos por severidade, eventos por regra, eventos por tendência e eventos por categoria;

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

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

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

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

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

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

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

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

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

3.2.43.12. 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;

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

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

3.2.43.15. 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;

3.2.43.16. 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;

3.2.43.17. 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;

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

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

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

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

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

4. **Item 2 - Serviço de Licenciamento e Garantia da Solução Implantada**

4.1 Acesso por 12 meses há:

4.1.1. Acesso a todas as Atualizações de Software incluindo atualizações de funcionalidades, patches de segurança e correções de bugs;

4.1.2. Substituição Avançada de Hardware (Advance RMA);

4.1.3. Assistência Proativa para Manutenções Programadas;

4.1.4. Base de Conhecimento AskF5;

4.1.5. Acesso ao fabricante por telefone e portal MyF5;

4.1.6. As solicitações deverão ocorrer através de abertura de chamado técnico, via serviço telefônico de Discagem Direta Gratuita (DDG) 0800 ou acesso web (e-mail, chat e/ou canais de comunicação), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

5. **Item 3 - Serviço de Suporte 12 meses**

5.1. A contratada deverá realizar a instalação de toda solução adquira pelo prazo máximo de 90 dias, após o recebimento da solução;

5.2. Deverá ser fornecido Relatórios de Pré-Requisitos de Instalação e Operação dos Produtos, contendo, por produto, informação de todos os seus pré-requisitos instalação e operação, a citar: conexões lógicas necessárias para interligação da solução com o ambiente proposto pelo Senac;

5.3. Deverá ser efetuado levantamento de requisitos, coletando-se informações do ambiente computacional do Senac, por meio de reuniões e verificações in-loco, com o objetivo de documentar e analisar informações quanto aos componentes de infraestrutura bem como estabelecer os parâmetros necessários à configuração e integração dos produtos;

5.4. Deverá ser entregue documentação de instalação de toda solução adquirida em modelo As-Built, descriminando todos os componentes da solução.

5.5. A instalação deverá ser executada e planejada por profissionais certificados, contendo no mínimo:

5.5.1. Um profissional certificado da solução, de nível intermediário do fabricante.

5.5.2. Um profissional certificado da solução, de nível mais avançado (especialista) do fabricante.

5.6. A implantação da solução deve ser realizada de acordo com as melhores práticas da indústria de TI;

5.7. A equipe operacional deve seguir as qualificações exigidas na habilitação técnica;

5.8. Após a instalação, o Senac deverá prestar acompanhamento da solução pelo período de 07 dias, a fim de verificar o comportamento da solução com relação às aplicações protegidas;

5.9. O serviço de suporte a ser prestado pela contratada tem por objetivo a correção de falhas ou inconsistências detectadas, de forma a garantir o pleno e correto funcionamento da solução;

5.10. Para chamados classificados com criticidade baixa e média, o profissional deverá possuir certificação em nível intermediário que comprove habilidade em administrar, integrar e/ou implantar solução no ambiente da SENAC;

5.11. Para chamados classificados com criticidade alta, o profissional deverá possuir certificação de nível avançado (especialista) da solução;

5.12. O serviço compreende auxílio na configuração das funcionalidades contratadas, esclarecimento de dúvidas e restabelecimento do serviço;

5.13. As solicitações deverão ocorrer através de abertura de chamado técnico, via serviço telefônico de Discagem Direta Gratuita (DDG) 0800 ou acesso web (e-mail, chat e/ou canais de comunicação), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

5.14. A abertura de cada chamado deverá receber um identificador único;

5.15. A contratada poderá efetuar um número ilimitado de chamados técnicos, devendo a SENAC cumprir o SLA no prazo estipulado neste instrumento;

5.15.1. Toda a oferta deverá possuir no mínimo 12 (doze) meses de garantia e suporte técnico do(s) seu(s) respectivo(s) fabricante(s) e da CONTRATADA.

5.15.2. Os chamados de suporte técnico serão classificados por níveis de severidade de acordo como impacto no ambiente computacional da SENAC, de acordo com as tabelas abaixo de Níveis de Severidade:

5.15.3. Prazos de Atendimento:

Níveis Mínimos de Serviço

Criticidade	Descrição	Prazo de Atendimento	
		Tempo de Resposta	Tempo de Conclusão
Alta	Os chamados classificados com criticidade "Alta" são definidos pela situação emergencial ou indisponibilidade total dos serviços.	2h	6h
Média	Os chamados classificados com criticidade "Média" são definidos pela indisponibilidade parcial ou mal funcionamento de alguns serviços.	4h	24h
Baixa	Os chamados classificados com criticidade "Baixa", são definidos pela situação não emergencial, geração de dúvidas e validações de configurações ou manutenções de baixo impacto.	12h	48h

5.15.4. Entende-se por início de atendimento, o momento da abertura do chamado técnico.

5.15.5. Entende-se por término de atendimento a disponibilidade da solução implementada para uso em perfeitas condições de funcionamento no local onde está instalada.

5.15.6. O nível de severidade será informado pela SENAC no momento da abertura de cada chamado.

5.15.7. Nos casos específicos em que seja necessário o desenvolvimento de patches ou atualizações a nível de software, será admitida a execução das soluções de contorno até que seja desenvolvida uma nova versão de correção do problema.

5.15.8. Uma vez disponível, a CONTRATADA deverá auxiliar a SENAC com todo o processo de atualização seguro da solução.

5.15.9. O nível de severidade poderá ser reclassificado a critério da SENAC. Caso isso ocorra, haverá o início de nova contagem de prazo, conforme o novo nível de severidade.

5.15.10. Depois de iniciado o atendimento, o mesmo não deverá ser interrompido até a recuperação do funcionamento dos serviços, salvo os casos em que a SENAC autorizar.

5.15.11. Quando um chamado não for solucionado no prazo máximo estabelecido, a equipe ou o técnico da CONTRATADA deverá permanecer no atendimento até a completa solução de contorno do problema, sem ônus adicional para a SENAC, independentemente da aplicação de multas e penalidades contratuais.

5.15.12. Nestes casos deve ser respeitado o horário de expediente da SENAC, salvo se houver o acompanhamento e a ordem expressa da fiscalização do contrato para que os integrantes da Contratada permaneçam no local.

5.15.13. Quando houver um chamado aberto e pendente de solução que independa da Contratada, nos casos em que a atividade ensejar parada de serviço de rede ou no caso de existirem serviços essenciais que não possam ser paralisados, o trabalho poderá ser realizado após o horário estabelecido. Neste caso, a Contratada não será penalizada.

5.15.14. A execução dos serviços deve ocorrer conforme programação identificada nas Ordens de Serviço, que serão abertas quando demandado pelo SENAC à CONTRATADA.

5.15.15. Quando os incidentes não forem sanados por meio de assistência remota, a CONTRATADA deverá realizar a atividade de forma presencial On-Site, respeitando o acordo de ANS desde a abertura dos chamados, conforme tabela níveis mínimos de serviço.

5.15.16. Em casos aos quais sejam constatados defeito de hardware e/ou necessidade de troca de peças ou de equipamentos, a reposição deverá ser acordada junto ao SENAC.

5.15.17. O suporte técnico mensal poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração com os dispositivos do SENAC, além do desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:

5.15.18. Orientação sobre acesso, o uso, a configuração, a instalação da solução e a integração com os dispositivos do SENAC, contando com acesso ao conhecimento privilegiado de recursos da CONTRATADA e quando necessário do FABRICANTE da solução.

5.15.19. Orientação quanto às melhores práticas para implementação e integração da solução no ambiente do SENAC.

5.15.20. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução;

5.15.21. Análise técnica qualificada nas análises e prevenções de vulnerabilidades encontradas e passíveis de serem exploradas;

5.15.22. Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático caso aconteçam.

5.15.23. Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas.

5.15.24. Parametrização da solução, de acordo com as regras e políticas definidas pele SENAC.

5.15.25. Apoio para execução de procedimentos de atualização de versão

5.15.26. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário.

5.15.27. Suporte avançado para estratégia e planejamento de migrações.

5.15.28. Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas a solução e seus componentes.

6. **Item 4 - Treinamento**

6.1.1. Deverá ser realizado treinamento do tipo repasse de conhecimento, não sendo necessário ofertar treinamento oficial do fabricante da solução, entretanto, o treinamento deverá ser realizado por instrutor certificado pelo fabricante;

6.1.2. O treinamento deverá ser ministrado para uma turma de até 05 alunos, nas dependências da SENAC ou em formato EAD.

6.1.3. A SENAC deverá disponibilizar uma sala adequada para o treinamento, contendo mesas e cadeiras suficientes para a quantidade de alunos, devendo também disponibilizar projetor.

6.1.4. A Contratada será responsável pelo fornecimento de material didático relativo à solução.

6.1.5. O treinamento deverá possuir uma duração mínima de 20 horas, devendo contemplar aspectos de instalação, configuração, administração e manutenção.

6.1.6. Deverá ser emitido certificado de participação individual no treinamento para alunos que possuírem frequência mínima de 70%.

Informações Complementares

Prazo de Garantia **12 Meses**
Prazo de validade da proposta comercial **90 Dias**
Condições de Pagamento **30 Dias**
Prazo de Entrega **120 Dias**

7. **VIGÊNCIA**

7.1. A vigência será de 12 (doze) meses para os itens 2 e 3, a partir do recebimento do Acordo de Compra, podendo:

7.1.1. ser prorrogada automaticamente, caso não haja manifestação em contrário de quaisquer das Partes com antecedência mínima de 60 (sessenta) dias, até o limite máximo de 60 (sessenta) meses, ou

7.1.2. ser denunciado pelas Partes, por escrito, a qualquer momento, com antecedência mínima de 30 (trinta) dias, ressalvando-se que, em até 2 (dois) úteis contados da data da comunicação escrita da denúncia, o Fornecedor procederá à devolução ao Senac do valor dos Serviços que ainda não tiverem sido executados se o Senac já tiver efetuado o pagamento.

7.2. O Acordo de Compra será considerado rescindido pelo Senac, de pleno direito, sem aviso prévio:

7.2.1. se a outra Parte entrar em liquidação voluntária ou compulsória, tornar-se insolvente ou falida ou requerer/for requerida sua insolvência, recuperação judicial ou extrajudicial ou falência e/ou for impedida/proibida de exercer suas atividades; ou

7.2.2. por motivo de força maior ou caso fortuito, na medida em que impossibilite total ou parcialmente o cumprimento das obrigações assumidas neste termo, ficando o Senac liberado do pagamento dos Serviços não executados.

7.3. O Fornecedor não poderá ceder ou transferir, parcial ou totalmente, as obrigações assumidas no presente processo sem a prévia e expressa autorização, por escrito, do Senac. Concedida referida autorização, o Fornecedor continuará responsável pelos Serviços contratados.

7.4. A sucessão contratual será permitida somente em decorrência de operações societárias de fusão, cisão ou incorporação realizada pelo Fornecedor e, desde que:

7.4.1. previamente analisada e consentida pelo Senac, considerando eventuais riscos ou prejuízos para o adimplemento contratual;

7.4.2. sejam mantidas todas as condições contratuais; e

7.4.3. exista expressa concordância do sucessor em assumir a responsabilidade pela execução do presente processo e receber os créditos dele decorrentes.

7.5. É vedada a cessão ou transferência parcial ou total de qualquer crédito, bem como a emissão, por parte do Fornecedor, de qualquer título de crédito decorrente do Acordo de Compra sem a prévia e expressa autorização, por escrito, do Senac.

8. Remuneração

8.1. O pagamento será realizado em única vez diretamente à Contratada em até 30 (trinta) dias após entrega dos produtos e início da prestação de serviços, através de emissão de nota fiscal e boleto bancário.

8.2. O **Fornecedor** deverá apresentar ao **Senac** a nota fiscal no prazo de 15 (quinze) dias antes do vencimento, visando ao atendimento da legislação aplicável em vigor.

8.3. A não efetivação do pagamento na forma e no prazo estabelecidos no presente Termo de Referência implicará na incidência de multa de 2% (dois por cento) do valor devido. Se o atraso for superior a 30 (trinta) dias, incidirão também juros de 6% (seis por cento) ao ano, calculados "pro-rata-mês", bem como atualização monetária pelo IGP-M/FGV calculada "pro-rata-die" até a data de seu efetivo pagamento.

8.4. O **Senac** poderá reter o(s) pagamento(s) previsto(s) na proposta comercial nas seguintes hipóteses:

i. se **o Fornecedor** não encaminhar as notas fiscais para o endereço correto e em tempo hábil;

ii. se **o Fornecedor** deixar de apresentar os documentos exigidos neste processo ou nele sejam constatadas quaisquer irregularidades;

iii. se houver erro de faturamento ou divergência de valor;

iv. se **o Fornecedor** fornecer Serviços irregulares;

v. para cobrir as obrigações previdenciárias e trabalhistas incidentes na execução dos Serviços e/ou em eventuais Reclamações Trabalhistas; ou

vi. se existirem pendências de responsabilidade do **Fornecedor**.

8.5. O valor homologado para os **ITENS 2 e 3** permanecerão inalterados pelo prazo de 12 (doze) meses contados da assinatura do presente Acordo de Compra, podendo ser reajustado após esse prazo, mediante solicitação do Fornecedor, pelo percentual da variação acumulada do IPCA apurado no período.

8.5.1. O índice fixado para o reajuste será o mesmo para toda a vigência, salvo se ocorrer a sua extinção, quando então as Partes poderão acordar outro índice para substituí-lo.

8.5.2. Será considerado para a concessão do reajuste o período dos últimos 12 (doze) meses anteriores ao mês de solicitação do reajuste feita pelo **Fornecedor.**

8.5.3. O valor homologado poderá ser revisto a qualquer tempo caso uma das Partes, considerando-se prejudicada, comprove inequívoco desequilíbrio econômico-financeiro que torne inviável a relação contratual.

8.5.4. Todos os encargos sociais, fiscais, trabalhistas, previdenciários e de acidente do trabalho correrão por conta do **Fornecedor**, nenhuma responsabilidade cabendo ao **Senac.**

8.5.5. Eventuais retenções na fonte de referidos encargos serão realizadas pelo **Senac**, na forma da legislação em vigor.

8.6. Estão incluídas no valor do presente Acordo de Compra todas as despesas decorrentes da execução dos Serviços.

9. **Multa**

9.1. Fica estipulada multa correspondente 10% (dez por cento) do valor total do Acordo de Compra, sem prejuízo de indenização suplementar pelos danos comprovadamente causados, na qual incorrerá a parte que infringir quaisquer cláusulas deste termo, excetuada:

i. a hipótese de atraso no pagamento, para a qual a penalidade está prevista no **Item 5.3** deste Termo de Referência e;

ii. eventuais penalidades específicas previstas em Anexos relacionadas a execução dos Serviços, não limitadas a Níveis Mínimos de Serviço e/ou avaliações, facultando-se, ainda, à Parte inocente o poder de considerar simultaneamente rescindido o presente instrumento, independentemente de qualquer notificação ou interpelação judicial ou extrajudicial.

9.2. Os termos e condições deste termo somente poderão ser alterados por meio de termo de aditamento escrito e:

i. de acordo com a vontade das Partes ou;
ii. em caso de determinação ou nova regulamentação da Autoridade Nacional de Proteção de Dados ("ANPD") relativamente às cláusulas que regulam o tratamento de dados pessoais.

10. **Documentação**

10.1. Durante a execução do contrato a solução fornecida não deve estar relacionada em listas "end of sale" e "end of support" do site do(s) fabricante(s).

10.2. Todas as licenças, referentes aos softwares e/ou componentes da solução adquirida, devem estar em nome do SENAC, legalizado, não sendo admitidas versões "shareware" ou "trial".

10.3. Deverão ser fornecidos todas as documentações e manuais técnicos completos necessários à instalação, configuração e operação dos componentes da solução de segurança de borda.

10.4. A documentação e manuais técnicos deverão estar em português ou inglês. Deverão ser fornecidos materiais técnicos e manuais em formato digital que permita a importação para base de conhecimento online (Microsoft Word, PDF, HTML, etc.);

10.5. O vencedor da licitação deverá deixar documentação completa das configurações dos equipamentos, bem como arquivos de backup de restauração das referidas configurações.

11. Entrega

11.1. Rua Dr. Vila Nova, 228, 10° andar (Datacenter Sede).

11.2. Até 120 (cento e vinte) dias a partir do recebimento do acordo de compra;

11.3. A solução como um todo deve ser fornecida e instalada, com todos os softwares, componentes ativados prontos para o uso;

11.4. Qualquer problema na entrega, configuração e ativação dos equipamentos deverão ser reportados imediatamente ao SENAC.

11.5. Os problemas originados nos componentes que estão sendo fornecidos devem ser resolvidos pela CONTRATADA dentro do prazo estabelecidos constantes neste Termo de Referência.

11.6. O preço proposto para este fornecimento deve englobar os valores relativos a impostos, fretes, seguros, salários, encargos e demais despesas necessárias ao fornecimento completo do objeto;

11.7. Para o aceite, a solução e seus componentes serão submetidos, a critério do SENAC, contemplando testes de desempenho e/ou demonstrações de funcionamento, que verificarão funções e parâmetros especificados neste Termo de Referência.

11.8. Caso a CONTRATADA necessite de tempo maior que 120 (cento e vinte) dias para entrega, a CONTRATADA deverá comunicar as razões respectivas com pelo menos 10 (dez) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado.

11.9. O prazo de entrega da solução como um todo é de 120 (cento e vinte) dias corridos conforme as condições de execução do contrato descritas no Termo de Referência.

12. **Garantia**

12.1. Mínima de 12 (doze) meses;

Gerência de Materiais e Serviços
Senac São Paulo

Rua Dr. Vila Nova, 228 7º andar
CEP 01222-903 — São Paulo / SP — Brasil
gms@sp.senac.br
www.sp.senac.br