SERVIÇO SOCIAL DA INDÚSTRIA – SESI
SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI
DEPARTAMENTO REGIONAL DE SÃO PAULO

CHAMAMENTO PÚBLICO

PROCESSO DE SELEÇÃO COM DISPUTA ABERTA

N.º 494/2026

OBJETO:
CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO, INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE DO TIPO *NEXT GENERATION FIREWALL* (NGFW) E RECURSOS DE SEGURANÇA, PARA ATENDIMENTO DAS NECESSIDADES DO SESI-SP E DO SENAI-SP

DATA DA DISPUTA: 19/11/2026 ÀS 14h30 (HORÁRIO DE BRASÍLIA)

CRITÉRIO DE SELEÇÃO: ECONÔMICO (MENOR PREÇO)

GERÊNCIA DE COMPRAS

SUMÁRIO

1. NORMAS ESPECÍFICAS....3
2. DO OBJETO....3
3. DA PARTICIPAÇÃO....4
4. DA APRESENTAÇÃO DA PROPOSTA NA PLATAFORMA ELETRÔNICA....5
5. DA FASE DE DISPUTA....7
6. DA PROPOSTA ESCRITA FINAL....9
7. DA DOCUMENTAÇÃO DE QUALIFICAÇÃO....9
8. DA ACEITAÇÃO DAS PROPOSTAS....11
9. DA ANÁLISE E JULGAMENTO DAS PROPOSTAS E DA DOCUMENTAÇÃO DE QUALIFICAÇÃO....12
10. DOS PEDIDOS ESCLARECIMENTOS E DE RECONSIDERAÇÃO....13
11. DA CONTRATAÇÃO....14
12. OBRIGAÇÕES DA CONTRATADA....17
13. DA GARANTIA DE EXECUÇÃO CONTRATUAL....18
14. ACORDOS DE NÍVEIS DE SERVIÇOS - ANS....19
15. DO PAGAMENTO....19
16. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES....21
17. CASOS OMISSOS....22

PROCESSO DE SELEÇÃO COM DISPUTA
FORMA ABERTA - Nº 494/2026

1. NORMAS ESPECÍFICAS

1.1. O presente documento, denominado "**Chamamento Público**" poderá ser obtido por meio dos endereços eletrônicos do Serviço Social da Indústria – SESI: https://transparencia.sesisp.org.br/licitacoes/licitacoes-editais e do Serviço Nacional de Aprendizagem Industrial – SENAI: https://transparencia.sp.senai.br/licitacoes/licitacoes-editais , ou na plataforma eletrônica: https://licitacoes-e2.bb.com.br/aop-inter-estatico/ na qual ocorrerá a disputa de preços, sob o **número 1103871.**

1.2. As regras para processamento da disputa serão as mesmas utilizadas na referida plataforma, salvo disposto em contrário neste instrumento, diferenciando-se apenas no que diz respeito às terminologias.

1.3. As normas deste Chamamento Público serão interpretadas em favor da ampliação da disputa entre as participantes.

1.4. Este Processo de Seleção poderá ser justificadamente cancelado, no todo ou em parte, a qualquer momento, bem como, ter seus prazos prorrogados, a critério da Comissão de Contratação.

2. DO OBJETO

2.1. O presente Processo de Seleção tem por objeto a contratação de empresa especializada para fornecimento, treinamento, instalação, configuração e migração de solução de segurança de rede do tipo *Next Generation Firewall (*NGFW*)* e recursos de segurança, da fabricante *FORTINET*, para atendimento das necessidades do SESI-SP e do SENAI-SP, conforme Memorial Descritivo e demais anexos.

2.1.1. Critério de seleção: **Econômico – menor preço**

2.1.2. Forma do Processo de Seleção: **Com disputa aberta**

2.1.3. Vigência Contratual: **05 (cinco) anos,** a contar da assinatura sem possibilidade de reajuste de preços, **exceto o item 03**, constante do item 4.2 - Lista de Materiais do Memorial Descritivo – Anexo B. A vigência contratual, se for o caso, desde que justificada e atendidas as previsões contidas nos artigos 34, II e 38 do RCA, poderá ser prorrogada até o limite máximo de 10 (dez) anos.

2.2. O Processo de Seleção será regido pelo **Regulamento para Contratação e Alienação – RCA** do Serviço Social da Indústria – SESI, aprovado pelo Conselho Nacional do SESI por meio da Resolução CN-SESI nº 0053/2023 e do Serviço Nacional de Aprendizagem Industrial – SENAI por meio da Resolução CN-SENAI nº 14/2023, de 16/05/2023, devidamente publicado no Portal da Transparência do SESI e do SENAI e pelas Normas Específicas contidas neste Chamamento Público e nos seguintes anexos:

Anexo A	Modelo de Declaração Concordando com os Termos do Chamamento Público e Outras Informações
Anexo B	Memorial Descritivo
Anexo C	Modelo de Proposta
Anexo D	Minutas de Contratos
Anexo E	Requisitos da Segurança e da Informação
Anexo F	Termo de Confidencialidade
Anexo G	Cronograma

2.3. **Definições**

2.3.1. **Contratante:** Serviço Social da Indústria – SESI e Serviço Nacional de Aprendizagem Industrial – SENAI, Departamento Regional de São Paulo.

2.3.2. **Comissão de Contratação:** formada por 3 membros, cuja atribuição é analisar, emitir pareceres técnico-financeiros, decidir acerca da qualificação dos participantes e das propostas, dos pedidos de reconsideração e do resultado do Processo de Seleção.

2.3.3. **Condutor:** um integrante da Comissão de Contratação que será o responsável pela condução da reunião de disputa, bem como das demais fases do processo.

2.3.4. **Participante:** empresa que apresentar proposta para o Processo de Seleção.

2.3.5. **Contratada:** empresa selecionada no Processo de Seleção.

3. DA PARTICIPAÇÃO

3.1. Poderão participar deste Processo de Seleção, empresas com ramo de atividade compatível com o objeto, comprovado por meio da Classificação Nacional de Atividade Econômica (CNAE), tal comprovação também poderá ser realizada por meio do Contrato Social.

3.2. Não poderão participar, empresas:

3.2.1. reunidas sob regime de Consórcio;

3.2.2. que possuam em seu quadro societário dirigente ou empregado do SESI-SP e SENAI-SP;

3.2.3. suspensas temporariamente do direito de contratar com o SESI-SP e o SENAI-SP;

3.2.4. declaradas inidôneas pelo Tribunal de Contas da União, site para consulta: https://contas.tcu.gov.br/ords/f?p=INABILITADO:INIDONEOS, nos termos do art. 46 da Lei nº 8.443/92;

3.2.5. estrangeiras que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

3.2.6. que estejam em processo de falência, em recuperação judicial ou extrajudicial, concursos de credores ou insolvência, em processo de dissolução ou liquidação;

3.2.6.1. as sociedades que se encontram em recuperação judicial ou extrajudicial deverão apresentar certidão positiva de recuperação judicial, com a respectiva comprovação da homologação judicial do plano de recuperação.

3.2.7. empresas em dissolução ou em liquidação, e

3.2.8. sociedades integrantes de um mesmo grupo econômico, assim entendidas como aquelas que possuam diretores, sócios, representantes legais ou responsáveis técnicos em comum e/ou utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesses comuns.

4. DA APRESENTAÇÃO DA PROPOSTA NA PLATAFORMA ELETRÔNICA

4.1. As empresas interessadas, portadores de chave e senha de acesso, deverão registrar propostas iniciais em conformidade com os requisitos definidos neste Chamamento Público, na plataforma eletrônica Novo Licitações-e: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, cuja reunião pública ocorrerá no dia e horário previsto no cronograma.

4.2. As interessadas deverão encaminhar a proposta escrita atualizada concomitantemente com a documentação de qualificação, conforme itens 6 e 7 deste Chamamento Público, EXCLUSIVAMENTE por meio do sistema eletrônico Novo Licitações-e: https://licitacoes-e2.bb.com.br/aop-inter-estatico/, em até 01 (um) dia útil após a solicitação.

4.3. Eventuais desistências e/ou alterações nas propostas iniciais registradas na plataforma deverão ser realizadas exclusivamente pelos participantes, antes da data e horário de abertura das propostas.

4.4. Será observado o horário de Brasília/DF para todas as referências de tempo contidas neste Chamamento Público.

4.5. A participação neste Processo de Seleção pressupõe o pleno conhecimento e atendimento às regras e exigências de qualificação previstas neste Chamamento Público, e na plataforma do Banco do Brasil, sendo responsável por todas as transações efetuadas.

4.6. Caberá a empresa participante acompanhar alterações de datas/horários, esclarecimentos, erratas e outras comunicações, bem como as operações no sistema eletrônico durante a reunião pública, inclusive das decisões da Comissão de Contratação, sendo responsável exclusivo pelo ônus decorrentes da perda de negócios diante da inobservância de quaisquer mensagens constantes da plataforma e ainda por eventuais perdas de conexão.

4.7. A disputa será conduzida pelo membro da Comissão de Contratação, denominado Condutor do Processo de seleção, que será responsável pelo seu processamento.

4.8. Os interessados em acompanhar a disputa poderão fazê-lo acessando na Internet o endereço eletrônico Novo Licitações-e hhttps://licitacoes-e2.bb.com.br/aop-inter-estatico/, onde se encontra o link do Processo Seletivo.

4.9. Ao cadastrar a proposta no *site* na plataforma eletrônica Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/, as informações inseridas no campo denominado "Descrição/Observação (Opcional)" tem caráter de preenchimento facultativo e não poderão identificar a empresa participante, visando preservar o sigilo das propostas.

4.10. Para elaboração da proposta a participante deverá considerar que:

4.10.1. O **preço total** dos serviços deve considerar os impostos diretos e indiretos, taxas, contribuições, fretes, seguros e quaisquer outras incidências fiscais e/ou tributárias e demais custos e despesas incidentes na prestação do serviço;

4.10.2. No caso de lotes com mais de um item, o valor total a ser lançado na plataforma eletrônica é a soma dos valores totais (quantidade x preço unitário) de cada item que compõe o lote;

4.10.3. Os preços cotados e os valores faturados, em moeda corrente nacional, deverão ser fixos e irreajustáveis, não sofrendo qualquer atualização monetária até o seu efetivo pagamento;

4.10.4. Validade mínima da proposta é de 90 (noventa) dias, contados da data disputa de preços.

4.10.5. A base dos preços será a data da disputa de preços.

4.10.6. Os serviços ofertados devem corresponder às exigências constantes do Memorial Descritivo e anexos, sob pena de desclassificação.

4.10.7. O pagamento será realizado no prazo definido no item **15 – DO PAGAMENTO**, não sendo aceita proposta com pagamento antecipado.

4.10.8. Pela elaboração da proposta a empresa participante não terá direito a auferir qualquer vantagem, remuneração ou indenização.

4.11. A proposta final e documentos de qualificação deverão ser anexados pela empresa arrematante, após a disputa, na plataforma Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/, no prazo de até 01 (um) dia útil após a solicitação do Condutor.

4.12. **Do Credenciamento na nova plataforma Licitações-e** https://licitacoes-e2.bb.com.br/aop-inter-estatico/ **.**

4.12.1. Para acesso ao sistema eletrônico, os interessados deverão dispor de chave de identificação e senha pessoal, ambas intransferíveis, obtidas junto ao provedor do sistema eletrônico (Banco do Brasil S/A).

4.12.2. As pessoas jurídicas ou empresas individuais deverão credenciar representantes, mediante a apresentação a referida instituição bancária (agência de livre escolha do interessado) de procuração por instrumento público ou particular, com firma reconhecida, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no sistema.

4.12.3. Em se tratando de sócio, proprietário ou dirigente da empresa interessada, deverá ser apresentada ao Banco do Brasil S/A cópia do respectivo Estatuto ou Contrato Social e alterações, no qual estejam expressos os poderes para exercer direitos e assumir obrigações.

4.12.4. A chave de identificação e senha terão validade determinada pelo Banco do Brasil S/A, sendo de exclusiva responsabilidade do usuário o sigilo, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao SESI-SP e ao SENAI-SP a responsabilidade por eventuais danos decorrente do uso indevido, ainda que por terceiros.

4.12.5. O credenciamento da empresa interessada e de seu representante legal junto ao sistema eletrônico implica na responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes.

5. DA FASE DE DISPUTA

5.1. A partir do horário previsto no cronograma será iniciada a reunião pública da disputa aberta de preços, cujos preços iniciais serão divulgados.

5.2. O Condutor realizará a disputa, podendo desclassificar as propostas que:

a) não estiverem em consonância com o exigido neste Chamamento Público, e

b) apresentem preços irrisórios ou incompatíveis com os preços de mercado, ainda que não se tenha estabelecido limite mínimo.

5.2.1. Tal decisão e outras pertinentes serão registradas na plataforma para acompanhamento das participantes.

5.2.2. A validade do processo de seleção não ficará comprometida, se inviabilizada a fase de lances, em razão da apresentação e/ou classificação de apenas uma empresa, desde que justificada pela Comissão de Contratação, inclusive quanto ao preço.

5.2.3. Aberta a etapa competitiva, os participantes deverão estar conectados ao sistema para participar da reunião de lances.

5.2.4. As empresas participantes poderão ofertar lances sem restrição de quantidade ou de qualquer ordem classificatória ou cronológica específica, mas sempre inferior ao seu último lance.

5.2.5. Todos os lances serão registrados pela plataforma, que indicará sempre o lance de menor valor para acompanhamento em tempo real pelas participantes, mantendo em sigilo os autores dos lances durante a reunião de disputa.

5.2.6. Será adotado para o envio de lances o modo de disputa “Aberto”, em que os participantes apresentarão lances públicos e sucessivos, com prorrogações.

5.2.7. Durante a disputa, as participantes deverão o valor mínimo de redução estabelecido para lances subsequentes, calculado com base em seu próprio lance anterior, conforme disposto a seguir:

LOTE	REDUÇÃO MÍNIMA ENTRE OS LANCES SUBSEQUENTES EM RELAÇÃO AO SEU LANCE ANTERIOR
01	R$ 10.000,00

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

5.2.8.1. A prorrogação automática da etapa de lances será de 02 (dois) minutos e ocorrerá sucessivamente, sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.2.8.2. Não havendo lances na forma estabelecida no item anterior, a sessão pública encerrar-se-á automaticamente.

5.2.9. A exclusão de lance somente será possível pelo fornecedor durante a fase de lances, dentro do prazo de 15 (quinze) segundos, conforme possibilita o sistema eletrônico, ou seja, antes do encerramento do lote.

5.2.10. No caso de desconexão do Condutor, durante a etapa de lances, se o sistema permanecer acessível aos participantes, os lances continuarão sendo recebidos sem prejuízo dos atos realizados.

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

5.2.12. Encerrada a disputa, o sistema informará a proposta de menor preço. O condutor do processo solicitará, no campo “*chat de mensagem*”, o envio da proposta escrita atualizada e documentos de qualificação correspondentes, para acesso público e avaliação do condutor, sendo necessariamente, inseridos pelo arrematante em até 01 (um) dia útil após solicitação na plataforma Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/ .

5.2.12.1. O Condutor poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao participante arrematante do lote, com vistas a redução do preço, decidindo sobre sua aceitação.

5.2.12.2. Caso o preço resultado desta negociação, ainda esteja incompatível com o mercado, o Condutor poderá convocar o participante subsequente para que tenha a mesma oportunidade e assim, sucessivamente.

5.2.13. A ausência da documentação, após o prazo de solicitação, ocasionará na desclassificação do participante e a convocação do próximo colocado em preço.

6. DA PROPOSTA ESCRITA FINAL

6.1. A proposta final deverá ser encaminhada pela arrematante, no prazo estabelecido no item 4.11. deste Chamamento Público, o qual poderá ser prorrogado por igual período a critério da Comissão de Contratação, devendo neste caso, ser utilizado o mesmo critério para as demais participantes.

6.2. Os documentos referentes a proposta escrita final são:

6.2.1. Modelo de declaração concordando com os termos do Chamamento Público e outras informações, Anexo A, credenciando o representante legal perante o SESI-SP e SENAI-SP para todos os assuntos pertinentes ao presente Processo de Seleção, entre outros.

6.2.2. Proposta de preços, com identificação da participante e do lote, conforme Modelo de Proposta, **Anexo C.**

6.3. O preço da proposta comercial escrita deverá ser o mesmo ofertado por lance durante a disputa eletrônica, salvo se houver tratativas realizadas com o Condutor, para obtenção de preço menor.

6.4. A proposta e a documentação de qualificação da arrematante serão analisadas pela Comissão de Contratação, que poderá se valer de assessoramento da área técnica e jurídica do SESI-SP e SENAI-SP, quando for o caso, podendo ser realizadas diligências para confirmação das informações contidas nos documentos apresentados e o atendimento as especificações exigidas, por meio de esclarecimentos ou informações complementares.

6.5. A inobservância da exigência, no prazo de 02 (dois) dias úteis, resultará na desclassificação da proposta para o lote correspondente.

6.6. A arrematante deve-se atentar ao item 8 deste chamamento para fins de aceite quanto a precificação dos serviços a serem contratados, objeto do presente processo de seleção.

7. DA DOCUMENTAÇÃO DE QUALIFICAÇÃO

7.1. **Modelo de Declaração Concordando com os Termos do Chamamento Público e Outras Informações, Anexo A,** concordando com os termos do Chamamento Público, autorizando o uso da imagem e tratamento dos dados, credenciando o representante legal perante o SESI-SP e SENAI-SP para todos os assuntos pertinentes ao presente Processo de Seleção, entre outros.

7.2. Prova de inscrição e de situação cadastral ativa no **Cadastro Nacional de Pessoas Jurídicas (CNPJ).**

7.3. Prova de inscrição no **Cadastro de Contribuinte Estadual**, relativa ao domicílio ou sede da participante, pertinente ao seu ramo de atividade e compatível com o objeto a ser contratado.

7.4. Prova de inscrição no **Cadastro de Contribuinte Municipal**, relativa ao domicílio ou sede da participante, pertinente ao seu ramo de atividade e compatível com o objeto a ser contratado.

7.5. Prova de **regularidade com a Fazenda Nacional** (certidão negativa de débitos relativos aos tributos federais e à Dívida Ativa da União), que abrangem as contribuições previdenciárias.

7.6. Prova de **regularidade para com a Fazenda Estadual**, do domicílio ou sede do participante, consubstanciada na Certidão expedida pela Secretaria de Estado dos Negócios da Fazenda e/ou Procuradoria Geral do Estado.

7.7. Prova de **regularidade para com a Fazenda Municipal**, referente a tributos mobiliários do domicílio ou sede do participante.

7.8. Prova de **regularidade relativa ao Fundo de Garantia por Tempo de Serviço - FGTS**, do domicílio ou sede da participante.

7.9. **Certidão Negativa específica de Falência**, Recuperações Judiciais e Extrajudiciais, expedida pelo Cartório Distribuidor do local da sede da pessoa jurídica, com data de emissão não anterior a 90 (noventa) dias contados da data da reunião pública, no caso de não constar prazo de validade em seu texto.

7.9.1. As sociedades que se encontram em recuperação judicial ou extrajudicial deverão apresentar certidão positiva de recuperação judicial, com a respectiva comprovação da homologação judicial do plano de recuperação.

7.10. **Registro comercial**, no caso de empresa individual, além da cópia do RG e CPF do titular.

7.10.1. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores. Os documentos deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

7.10.2. Inscrição do ato constitutivo, no caso de sociedades simples ou civis, acompanhada de prova da diretoria em exercício.

7.11. **Aptidão Técnica**

7.11.1. **Atestado/Declaração de capacidade técnica**, expedida por pessoa jurídica de direito público ou privado, na qualidade de contratante para o qual prestou serviços objeto da presente contratação.

I. O(a) atestado(s)/declaração(ões) em papel timbrado do cliente, deverá(ão) conter:

a) Razão Social, CNPJ, endereço e contato do emitente;

b) Razão Social, CNPJ, endereço e contato da empresa contratada;
c) Objeto compatível com esta contratação;
d) Data de início da prestação dos serviços;
e) Histórico dos serviços prestados;
f) Data da emissão; e
g) Assinatura e identificação do responsável pela declaração.

II. O(a) atestado(s)/declaração(ões) deverá conter ainda:

a) A solução de firewall deverá ser do tipo Next Generation Firewall (NGFW), contemplando **funcionalidades e características técnicas compatíveis com o objeto desta contratação**, devendo possuir suporte, atualizações de segurança e recursos tecnológicos compatíveis.
b) Prestação de serviços de suporte técnico especializado, manutenção preventiva e corretiva, além de atualização e revisão de software (firmware) em soluções de NGFW;

7.11.2. Os requisitos acima poderão ser comprovados por meio de um único atestado de capacidade técnica ou por meio de atestados distintos, que poderão ser considerados de forma conjunta, desde que o conjunto dos documentos apresentados demonstre, de forma clara e inequívoca, que a participante possui **experiência compatível com o fornecimento e/ou a execução dos serviços relacionados ao objeto da contratação.**

7.12. Os documentos de qualificação, bem como quaisquer outros solicitados, deverão estar válidos na data da entrega.

7.13. Serão aceitas certidões positivas com efeito de negativa.

8. DA ACEITAÇÃO DAS PROPOSTAS

8.1. A critério da Comissão de Contratação, poderão ser relevados erros ou omissões formais, de que não resultem prejuízo para o entendimento das propostas.

8.2. Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado.

8.3. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, de acordo com o que estabelece o item 9.4., para efeito de comprovação de sua exequibilidade, no prazo máximo de 02 (dois) dias úteis após a solicitação.

8.3.1. O resultado da oitiva será submetido a Comissão de Contratação para análise e deliberação.

8.3.2. O não atendimento à solicitação no prazo fixado ou a recusa em fazê-lo implicará na desclassificação da proposta.

8.4. Será desclassificada a proposta que não corrigir ou não justificar eventuais falhas apontadas.

9. DA ANÁLISE E JULGAMENTO DAS PROPOSTAS E DA DOCUMENTAÇÃO DE QUALIFICAÇÃO

9.1. A Comissão de Contratação poderá se valer de assessoramento técnico para análise das propostas e documentação de qualificação apresentadas pelas participantes, os quais emitirão pareceres que subsidiarão as tomadas de decisões.

9.2. A critério da Comissão de Contratação, eventuais falhas ou omissões formais poderão ser relevados, desde que não resultem em prejuízo para o entendimento das propostas.

9.3. Não serão aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos requeridos no presente Chamamento Público.

9.4. Durante o Processo de Seleção, é facultado a Comissão de Contratação ou aos técnicos por ela designados realizar diligências para esclarecimentos e informações complementares, bem como conceder prazo para que os participantes adequem suas propostas e documentos de qualificação, visando sanar eventuais omissões ou inadequações.

9.4.1. A critério da Comissão de Contratação poderão ser aceitos documentos que, embora não entregues quando da convocação, estavam vigentes e/ou válidos na data da solicitação.

9.5. Todos os cálculos serão efetuados com duas casas decimais, desprezando-se sempre a fração remanescente.

9.6. A análise das propostas, observará a ordem da classificação, resultante da disputa de preços, restringindo-se, a princípio, à proposta apresentada pela arrematante, desde que atenda plenamente as exigências deste Chamamento Público, caso contrário, será avaliada a proposta subsequente e assim sucessivamente, até a obtenção de proposta válida.

9.6.1. Visando à celeridade do processo, a critério da Comissão de Contratação, poderá ser solicitada proposta final das próximas colocadas, para análise simultânea e concomitantemente.

9.7. O Condutor poderá negociar com as participantes, observando a ordem de classificação das propostas, visando a redução dos preços e adequação ao mercado.

9.8. Serão desclassificadas as participantes:

9.8.1. nas situações previstas no item 3.2;

9.8.2. cujas propostas não atendam às exigências constantes do Memorial Descritivo;

9.8.3. na apresentação de declarações emitidas por empresas que mantenham vínculo societário ou qualquer outra forma de relação direta ou indireta com a participante, tais como participação comercial, técnica, econômica ou financeira;

9.8.3.1. No caso de apresentação de atestado de capacidade técnica emitido por empresa integrante do mesmo grupo econômico da participante, a Comissão de Contratação poderá realizar, diretamente ou por meio de técnicos por ela designados, diligências destinadas à obtenção de esclarecimentos e informações complementares, bem como conceder prazo para que a participante apresente cópias de contratos, medições, notas fiscais ou outros documentos que comprovem a efetiva execução dos serviços e a aptidão técnica declarada.

9.8.4. que deixarem de apresentar os documentos solicitados nos itens 6. DA PROPOSTA ESCRITA FINAL E 7. DA DOCUMENTAÇÃO DE QUALIFICAÇÃO, **exceto do Anexo A** - visto que a entrega da proposta implica na aceitação formal das condições estabelecidas neste Chamamento Público.

9.9. O não atendimento aos requisitos e dos prazos estipulados neste Chamamento Público, a participante será desclassificada, cabendo ao Condutor registrar e disponibilizar a decisão no sistema eletrônico para acompanhamento em tempo real pelas participantes.

9.10. Caso haja desistência da proposta, a critério exclusivo do SESI-SP e SENAI-SP, a participante poderá ser penalizada com a suspensão do direito de contratar com o SESI-SP e SENAI-SP, por um período de até 05 (cinco) anos.

9.11. Constatado o atendimento dos requisitos previstos neste Chamamento Público, a participante será classificada e considerada apta para contratação.

9.12. Caso haja empate entre duas ou mais propostas, prevalecerá a primeiramente registrada, desde que tenha atendido a todos os requisitos exigidos neste Chamamento Público.

9.13. Na hipótese de desclassificação de todos os participantes, o SESI-SP e SENAI-SP poderão fixar novo prazo para apresentação de outras propostas ou de novos documentos, escoimados das causas que implicaram na desclassificação.

9.14. O resultado dessas análises será submetido à Comissão de Contratação, sendo as decisões lavradas em atas e disponibilizadas às participantes na plataforma Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/, abrindo-se o prazo para apresentação de pedido de reconsideração.

10. DOS PEDIDOS ESCLARECIMENTOS E DE RECONSIDERAÇÃO

10.1. As eventuais dúvidas deverão ser encaminhadas, até a data prevista no cronograma anexo, através do *e-mail* contservicos@sesisenaisp.org.br, *à* Gerência de Compras – GC, mencionando o número do Processo de Seleção e o objeto da contratação.

10.2. As respostas, eventuais esclarecimentos e/ou alterações serão disponibilizadas às interessadas nos endereços eletrônicos do Serviço Social da Indústria – SESI: https://transparencia.sesisp.org.br/licitacoes/licitacoes-editais e do Serviço Nacional de Aprendizagem Industrial – SENAI: https://transparencia.sp.senai.br/licitacoes/licitacoes-editais , e na plataforma eletrônica: https://licitacoes-e2.bb.com.br/aop-inter-estatico/ até a data prevista no

cronograma, sem, porém, identificar o formulador da consulta, as quais passarão a valer como normas.

10.3. Das decisões proferidas quanto a qualificação das participantes e de suas propostas, caberá pedido de reconsideração à Comissão de Contratação, no prazo de 02 (dois) dias úteis após a divulgação do resultado de cada participante, na plataforma do Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/, a ser encaminhado através do e-mail: contservicos@sesisenaisp.org.br.

10.3.1. As participantes, cuja situação no processo possa ser afetada, poderão se manifestar sobre o pedido de reconsideração, no prazo de 02 (dois) dias úteis, a contar da divulgação do resultado na plataforma do Novo Licitações-e https://licitacoes-e2.bb.com.br/aop-inter-estatico/.

10.3.2. Havendo pedido de reconsideração, o prazo de validade das propostas será suspenso, reiniciando-se a contagem a partir da divulgação do resultado.

10.4. Da decisão da Comissão de Contratação relativa ao pedido de reconsideração não caberá novo pedido de reconsideração.

10.5. Definido o resultado pela Comissão de Contratação e não havendo pedidos de reconsideração ou sendo estes devidamente analisados e respondidos, o Processo de Seleção seguirá para conclusão.

11. DA CONTRATAÇÃO

11.1. As condições estabelecidas neste Chamamento Público, no que se aplicar, farão parte do contrato e/ou pedido de compra correspondente, independentemente de transcrição em seu texto.

11.2. Após aprovação do Processo de Seleção, a participante selecionada será notificada para assinatura do contrato no prazo de 02 (dois) dias úteis, conforme a respectiva minuta, **Anexo D**.

11.2.1. A documentação de qualificação apresentada na plataforma eletrônica será utilizada para a realização do Cadastro da participante selecionada. Entretanto, quando da assinatura do contrato, poderá haver necessidade de atualização da documentação, em parte ou no todo, que deverá ser providenciada pela empresa a ser contratada, no prazo de até 02 (dois) dias úteis.

11.2.1.1. O prazo acima estabelecido poderá ser prorrogado, a critério exclusivo da Comissão de Contratação.

11.3. Caso a participante selecionada não assine o contrato e/ou não apresente a documentação regular, no prazo de até 02 (dois) dias úteis, a critério exclusivo do SESI-SP e SENAI-SP, a mesma poderá ser penalizada com a suspensão do direito de contratar com o SESI-SP e SENAI-SP, por um período de até 05 (cinco) anos e/ou aplicadas as penalidades previstas no item **16** - **DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES.** Nesse caso, o SESI-SP e SENAI-SP poderão convocar as participantes

remanescentes para fazê-lo, observada a ordem de classificação, ou realizar novo Processo de Seleção.

11.4. Antes da assinatura do contrato, o SESI-SP e SENAI-SP poderão desclassificar a participante selecionada, caso tenha conhecimento de qualquer fato anterior ou posterior ao julgamento deste Processo de Seleção que venha desaboná-la técnica, financeira ou administrativamente, não lhe cabendo direito a qualquer reclamação, indenização ou ressarcimento.

11.5. O futuro contrato vigorará pelo prazo de 05 (cinco) anos.

11.5.1. A vigência contratual, se for o caso, desde que justificada e atendidas as previsões contidas nos artigos 34, II e 38 do RCA, poderá ser prorrogada até o limite máximo de 10 (dez) anos.

11.6. A pedido da CONTRATADA, observando o subitem 11.6.1 abaixo, após o 12º mês de vigência contratual, poderá ser aplicado o reajustamento de preço anual com base no índice IPCA/IBGE acumulado nos últimos 12 meses, relativo ao mês anterior (11º mês), ou, mediante concordância entre as partes, referente ao segundo mês anterior ao 12º (10º mês), ou ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

11.6.1. **O reajustamento previsto no item 11.6. será aplicado exclusivamente ao item 03 da Lista de Materiais, do subitem 4.2, do Memorial Descritivo.**

11.7. Qualquer uma das partes poderá denunciar o futuro contrato antecipadamente, desde que comunique sua intenção com no mínimo 60 (sessenta) dias de antecedência.

11.8. Como condição para o início dos serviços, no prazo de até 05 (cinco) dias úteis após a assinatura do contrato, a Contratada deverá apresentar ao gestor do contrato do SESI-SP e do SENAI-SP a relação dos profissionais responsáveis técnicos alocados aos serviços, acompanhada dos respectivos documentos, contendo, obrigatoriamente:

I. Plano de Trabalho e Cronograma Detalhado, conforme subitem 5.2.1 do Memorial Descritivo (Anexo B);

II. Currículo(s) do(s) profissional(is) alocado(s) ao(s) serviço(s);

III. Cópia simples do(s) certificado(s) dos colaboradores alocados aos serviços, sendo exigida, no mínimo, 01 (uma) das certificações relacionadas abaixo, integrantes do programa de certificação do fabricante, em nível compatível com a implantação e administração das soluções ofertadas:

a) Certificação em nível profissional para atuação com NGFW e FortiManager; e
b) Certificação em nível especialista para atuação em projetos envolvendo SD-WAN e SASE.

Obs.: A(s) certificação(ões) apresentada(s) deverá(ão) permanecer válida(s) durante todo o período de execução dos serviços.

IV. Declaração emitida pela empresa, atestando que os profissionais designados para a execução dos serviços possuem, no mínimo, 03 (três) anos de experiência profissional nas atividades relacionadas às soluções objeto da contratação, contemplando, no mínimo:

a) **Arquitetura, configuração e operação de NGFW**, incluindo: configuração e administração de políticas de segurança; NAT; IPS; controle de aplicações; filtragem web; e inspeção de tráfego criptografado.
b) **Implementação de Secure SD-WAN**, incluindo: Performance SLA; Tuneis IPsec; BGP; e topologias *hub-and-spoke*.
c) **Utilização de ferramenta de gerenciamento centralizado**, contemplando: gerenciamento centralizado de dispositivos; utilização de *templates* e provisionamento; controle de mudanças; versionamento; e procedimentos de *rollback*; Conceitos e implantação de Zero Trust Network Access (ZTNA) e SASE, incluindo a integração entre as duas tecnologias; e Integração das soluções com ambientes *on-premises*, híbridos e em nuvem, bem como com usuários remotos.

Obs.: A declaração deverá identificar os profissionais designados para a execução dos serviços e informar o período de experiência de cada profissional, de forma a permitir a validação do atendimento.

V. Cópia do vínculo do(s) profissional(is) indicado(s) na relação com a estrutura organizacional da Contratada, podendo ser apresentada:

a) Para profissional registrado pela Contratada: cópia da CTPS ou ficha de registro; ou;
b) Para profissional contratado mediante prestação de serviços: cópia do contrato celebrado entre as partes.

11.8.1. Não haverá limite de profissionais alocados aos serviços, desde que o atendimento seja prestado com eficiência e em conformidade com as disposições deste processo de seleção.

11.8.2. A Contratada poderá substituir o profissional indicado na relação, desde que o novo profissional possua qualificações técnicas equivalentes às do substituído, devendo ser encaminhada ao gestor do contrato do SESI-SP e do SENAI-SP a documentação comprobatória de sua qualificação técnica, nos termos do item 11.8 deste Chamamento Público.

Justificativa: As exigências acima fundamentam-se na necessidade de assegurar que a CONTRATADA disponha de capacidade operacional e de corpo técnico devidamente qualificado, com experiência compatível com a complexidade da infraestrutura de redes e segurança da informação do SESI-SP e do SENAI-SP.
O ambiente tecnológico e a criticidade dos serviços envolvidos demandam profissionais devidamente qualificados, com conhecimentos técnicos e experiência comprovada nas tecnologias objeto da contratação, visando garantir a adequada execução dos serviços e atingir os seguintes objetivos fundamentais:

I. Garantia da Continuidade de Negócios e Cumprimento de SLAs: a infraestrutura de segurança suporta atividades críticas da instituição. Falhas operacionais ou indisponibilidades causadas por imperícia técnica podem paralisar operações essenciais, gerando prejuízos financeiros e institucionais incomensuráveis.

II. **Mitigação de Riscos Técnicos, Cibernéticos e Operacionais:** A correta configuração de políticas de segurança de última geração (NGFW), inspeção de tráfego criptografado e mitigação de intrusões (IPS) exige conhecimento especializado para evitar brechas de segurança, vazamento de dados ou incidentes cibernéticos.

III. **Otimização e Resiliência da Conectividade (Secure SD-WAN):** A implementação de topologias complexas (hub-and-spoke), roteamento dinâmico (BGP) e túneis IPsec com políticas de Performance SLA exige domínio prático para assegurar a alta disponibilidade dos links de comunicação, balanceamento eficiente de carga e resiliência perante falhas de operadoras.

IV. **Governança, Rastreabilidade e Alinhamento com Boas Práticas**: O uso adequado do gerenciamento centralizado (aplicação de templates, controle de versionamento e capacidade de rollback) e a adoção de conceitos modernos de arquitetura Zero Trust(ZTNA/SASE) garantem que o ambiente permaneça auditável, padronizado e estritamente aderente às recomendações e manuais do fabricante, maximizando o retorno sobre o investimento e a vida útil dos ativos de segurança.

12. OBRIGAÇÕES DA CONTRATADA

12.1. Executar os serviços, objeto deste Chamamento Público, de acordo com as exigências definidas no Memorial Descritivo, Minuta de Contrato e demais anexos.

12.2. Responsabilizar-se, em caráter exclusivo, pela execução dos serviços por seus empregados, prepostos, parceiros e terceiros.

12.3. Executar os serviços nos prazos estabelecidos no Memorial Descritivo, Minuta de Contrato e demais anexos.

12.4. Arcar com eventuais custos de transporte, estadia, alimentação entre outros, necessários à execução dos serviços.

12.5. Considerar a vistoria e aceitação dos serviços por técnicos do SESI-SP e SENAI-SP, se for o caso.

12.6. Notificar por escrito ao SESI-SP e SENAI-SP, ao gestor do Contrato, caso ocorra qualquer fato que impossibilite o cumprimento das condições e prazos estabelecidos no contrato.

12.7. Responsabilizar-se por todos e quaisquer danos e/ou prejuízos que venham a causar ao SESI-SP e SENAI-SP.

12.8. Solucionar eventuais falhas sem ônus ao SESI-SP e SENAI-SP.

12.9. Manter, durante o tempo de vigência do contrato, os documentos de regularidade fiscal e regularidade técnica devidamente atualizados.

12.10. Os serviços inerentes à esta contratação serão conduzidos sob a fiscalização da Gerência Sênior de Tecnologia da Informação do SESI-SP e do SENAI-SP, que indicará funcionário que exercerá a função de Gestor do Contrato, responsável por acompanhar a execução, as etapas e prazos determinados, conferir os documentos e relatórios pertinentes, atestar a realização dos serviços e liberar os pagamentos correspondentes.

12.11. Respeitadas todas as previsões descritas neste chamamento, no memorial descritivo e na minuta de contrato, a Contratada é a única e exclusiva responsável por todos os encargos trabalhistas, inclusive decorrentes de acordos, dissídios e convenções coletivas, previdenciários, fiscais e comerciais, oriundos da execução do contrato, podendo o SESI-SP e o SENAI-SP, a qualquer tempo, exigir a comprovação do cumprimento de tais encargos, como condição do pagamento do valor ajustado no contrato.

12.12. Sem prejuízo das demais documentações exigidas na minuta contratual, **caso haja prestação de serviços de forma presencial em estabelecimentos do SESI-SP e/ou SENAI-SP nos quais sejam atendidas ou estejam presentes crianças e adolescentes**, a CONTRATADA deverá emitir e encaminhar ao SESI-SP e/ou SENAI-SP, conforme o caso, a cada 06 (seis) meses, **certidões de antecedentes criminais atualizadas de seus colaboradores que atuem presencialmente nesses estabelecimentos**, em atendimento ao disposto no artigo 59-A do Estatuto da Criança e do Adolescente.

13. DA GARANTIA DE EXECUÇÃO CONTRATUAL

13.1. A participante deverá informar na proposta a ser apresentada, Anexo C, a modalidade de garantia de execução contratual, correspondente a 5% (cinco por cento) do valor total proposto anual, podendo ser escolhida entre as seguintes:

a) Caução em Dinheiro;
b) Fiança Bancária, e
c) Seguro Garantia.

13.2. No caso de Garantia de Execução Contratual, na modalidade “Caução em Dinheiro”, deverá ser efetuada no ato da assinatura do contrato, mediante comprovante de depósito, conforme dados abaixo:

Banco do Brasil: 001
Agência: 3221-2
Conta Poupança: 104.321-8
Variação: 51
Empresa: Serviço Social da Indústria – SESI
CNPJ: 03.779.133/0001-04

Banco do Brasil: 001
Agência: 3221-2
Conta Poupança: 1155-X
Variação: 51
Empresa: Serviço Nacional de Aprendizagem Industrial – SENAI
CNPJ: 03.774.819/0001-02

13.2.1. A devolução ocorrerá em até 30 (trinta) dias corridos, após a conclusão dos serviços, devidamente atualizado pela remuneração da caderneta de poupança, no período em questão.

13.3. No caso de Garantia de Execução Contratual, na modalidade "Fiança Bancária", esta deverá ser emitida por **Instituição Financeira legalmente autorizada pelo Banco Central** e apresentada no original ou meio eletrônico, com firma reconhecida e expressa renúncia aos benefícios dos artigos 827, 834, 835, 837, 838 e 839 do Código Civil, sendo o seu prazo de validade, no mínimo, igual ao prazo de vigência do contrato que será firmado pela participante selecionada.

13.4. No caso de Garantia de Execução Contratual na modalidade "Seguro Garantia", a apólice deverá ser emitida por uma **Companhia de Seguros legalmente autorizada pela SUSEP**, apresentada no original ou meio eletrônico, sendo seu prazo de vigência, no mínimo, igual ao prazo de vigência do contrato, que será firmado pela participante selecionada.

14. ACORDOS DE NÍVEIS DE SERVIÇOS - ANS

14.1. O SESI-SP e o SENAI-SP acompanharão o desempenho da Contratada no que diz respeito ao **Acordo de Nível de Serviço (ANS)**, também conhecido por **SLA (Service Level Agreement)**, quanto aos padrões de qualidade e desempenho durante a prestação dos serviços.

14.2. O SESI-SP e o SENAI-SP avaliarão o desempenho da Contratada e a qualidade dos entregáveis, no que respeita ao cumprimento dos Acordos de Níveis de Serviços – ANS e demais cláusulas contratuais e identificarão, quando for o caso, as inconformidades detectadas, notificando a Contratada acerca dos valores dos descontos aplicáveis no respectivo período, conforme quadro constante do item 7.1 do Memorial Descritivo (Anexo B), cabendo à Contratada promover o desconto correspondente.

15. DO PAGAMENTO

15.1. Os pagamentos serão efetuados em até 15 (quinze) dias corridos, contados da apresentação da respectiva nota fiscal/fatura, acompanhada dos relatórios técnicos e demais documentos necessários à validação dos serviços executados no período, fora a dezena, de modo que ocorram nos dias 10, 20 ou 30.

15.1.1. Quando essas datas recaírem em finais de semana ou feriados, o pagamento será efetuado no primeiro dia útil subsequente. No mês de fevereiro, os pagamentos serão realizados nos dias 10, 20 e 28, ou 29, em caso de ano bissexto.

15.1.2. O(s) pagamento(s) deverão ser rateados entre o SESI-SP e o SENAI-SP, observando-se a participação de cada entidade na contratação, na execução do objeto e na destinação dos itens e serviços, conforme definido neste processo de seleção, na proposta comercial e nos demais documentos contratuais aplicáveis.

15.1.3. Após a aceitação dos serviços pelo SESI-SP e SENAI-SP, a CONTRATADA deverá emitir faturas individuais para cada pedido de compra, conforme etapa concluída.

Etapa	Descrição da Execução	Prazo Estimado para a Execução	Valor a ser pago
1	Entrega e instalação dos equipamentos: • **FortiGate-201G** (item 01 do Anexo I) • **1GE SFP SX transceiver module** (item 05 do Anexo I) • **10GE SFP+ transceiver module, short range** (item 06 do Anexo I)	Até **15 (quinze) dias úteis** após o recebimento do respectivo Pedido de Compra.	Parcela única, correspondente a 50% do valor total contratado
2	Ativação das licenças/suporte, implantação, migração, conclusão do período de operação assistida e aceitação final da solução.	Até 30 (trinta) dias úteis após o recebimento do respectivo Pedido de Compra.	Parcela única, correspondente a 50% do valor contratado
3	Fornecimento: FortiManager - VM License	Conforme necessidade e ativação da licença, mediante Pedido de Compra.	Parcela Única
4	Fornecimento: FortiManager - VM FortiCare Premium Support for 5 years	Vigência de **60 (sessenta) meses**, conforme condições estabelecidas para o suporte contratado	Parcela Única
5	Treinamento Técnico	Conforme cronograma a ser definido entre as partes, após o recebimento do respectivo Pedido de Compra.	Parcela Única
6	Serviço de Implementação da solução / Migração	Conforme cronograma a ser definido entre as partes, após o recebimento do respectivo Pedido de Compra.	Parcela Única

15.2. Caso sejam identificadas pendências, inconformidades ou descumprimento de qualquer obrigação contratual, o pagamento poderá ser suspenso total ou parcialmente até a regularização, sem prejuízo da aplicação das penalidades cabíveis, inclusive glosas, quando previstas.

15.3. Para contagem do prazo de pagamento, considerar-se-á o dia da entrega da Nota Fiscal / Fatura, devidamente validada pelo Gestor do Contrato.

15.4. O SESI-SP e SENAI-SP, em conformidade com a legislação vigente, reterá do valor bruto da Nota Fiscal / Fatura, as alíquotas referentes aos impostos/taxas: IR, INSS, ISS, CSLL, COFINS, PIS/PASEP, entre outros, os quais deverão estar devidamente destacados no documento fiscal.

15.5. Os pagamentos serão efetuados através de depósito bancário, devendo ser encaminhadas, obrigatoriamente, as duplicatas e/ou recibos devidamente quitados. Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

15.6. A Contratada deverá aplicar os descontos decorrente das inconformidades detectadas pelo SESI-SP e pelo SENAI-SP, quando houver, em atendimento ao item 13.3. do Memorial Descritivo (Anexo B).

15.7. A CONTRATADA deverá manter, durante toda a vigência contratual, as condições de habilitação e regularidade exigidas para o recebimento dos valores contratados.

16. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

16.1. **À Participante:**

16.1.1. O não atendimento das exigências previstas neste Chamamento Público, dos compromissos assumidos, bem como, se for constatado inveracidade de quaisquer informações e/ou documentos fornecidos, poderá implicar, à participante, a penalidade de desclassificação da proposta e consequente exclusão do Processo de Seleção.

16.1.2. A recusa injustificada ou não aceita pelo SESI-SP e SENAI-SP em assinar o contrato e/ou os pedidos de compra, dentro do prazo fixado, caracterizará o descumprimento total das obrigações assumidas e poderá acarretar às seguintes penalidades:

a) perda do direito à contratação, e

b) suspensão do direito de contratar com o SESI-SP e SENAI-SP pelo prazo de até 05 (cinco) anos.

16.2. **À Contratada:**

16.2.1. Atrasos e/ou descumprimento de quaisquer obrigações pactuadas neste instrumento e demais obrigações constantes do PSDA nº 494/2026, acarretará a aplicação de multa no percentual de 2% (dois por cento) do valor do contrato.

16.2.2. A parte que der motivo à rescisão ou por descumprimento das cláusulas e condições pactuadas, ou ainda, após a entrega, restar provado que os serviços/materiais e/ou equipamentos não atenderam as especificações, incorrerá no pagamento, à parte inocente, da multa equivalente a 10% (dez por cento) do valor total do contrato, ressalvado o direito ao credor de exigir indenização por prejuízo excedente, nos termos do parágrafo único do art. 416 do Código Civil.

16.2.3. O inadimplemento total ou parcial das obrigações contratuais assumidas pela CONTRATADA, dará ao SESI-SP e ao SENAI-SP o direito de rescindir unilateralmente o contrato,

sem prejuízo de outras penalidades previstas, inclusive a de suspensão do direito de participar de processos de seleção junto ao SESI-SP e ao SENAI-SP por prazo não superior a 05 (cinco) anos, impedimento esse extensivo às pessoas físicas que constituíram a pessoa jurídica, as quais permanecem impedidas de participar enquanto perdurarem as causas da penalidade, independentemente de nova pessoa jurídica que vierem a constituir ou de outra em que figurem como sócios, e às pessoas jurídicas que tenham sócios comuns com as pessoas físicas acima mencionadas.

16.3. As penalidades previstas neste Contrato e no Memorial Descritivo são independentes, não excludentes e poderão ser aplicadas cumulativamente.

16.4. Os valores relativos às multas aplicadas, bem como outros valores que forem devidos pela CONTRATADA, poderão ser deduzidos dos créditos que possuir junto ao SESI-SP e ao SENAI-SP ou cobrados administrativa ou judicialmente.

17. CASOS OMISSOS

17.1. Qualquer caso omisso no decurso deste Chamamento Público será dirimido pela Comissão de Contratação e produzirá seus efeitos.

São Paulo, 10 de novembro de 2026.

Gerência de Compras – GC
Serviço Social da Indústria (SESI)
Serviço Nacional de Aprendizagem Industrial (SENAI)
Departamento Regional de São Paulo

ANEXO A

MODELO DE DECLARAÇÃO CONCORDANDO COM OS TERMOS DO CHAMAMENTO PÚBLICO E OUTRAS INFORMAÇÕES

(*em papel timbrado da participante)*

Ao
Serviço Social da Indústria (SESI)
Serviço Nacional de Aprendizagem Industrial (SENAI)
Gerência de Compras - GC

CHAMAMENTO PÚBLICO N. º 494/2026

DADOS DA EMPRESA	
Razão Social:	
Endereço completo:	
Telefone:	*E-mail*:
CNPJ:	

SÓCIOS E ADMINISTRADORES	
Nome:	Qualificação:
Nome:	Qualificação:

DADOS DO REPRESENTANTE LEGAL	
Nome:	Cargo:
CPF:	RG:
Telefone:	*E-mail*:

DADOS DO CONTADOR OU DA EMPRESA DE CONTABILIDADE		
Nome do Contador:		CRC:
Razão Social:	CNPJ:	CRC do responsável:

DADOS BANCÁRIOS DA EMPRESA PARA PAGAMENTO (se houver possibilidade de pagamentos em mais de uma conta, lista todas as possíveis)		
Banco:	Agência:	Conta Corrente:

Declaramos sob as penalidades da Lei, para fins do Processo de Seleção acima referido que:

a) concorda com as condições e regras deste Chamamento Público;
b) autorizo o uso de imagem e o tratamento dos dados;
c) na composição societária não existe participação de dirigentes ou empregados do SESI-SP e SENAI-SP;
d) na composição societária não existe participação de dirigentes ou sócios de qualquer outra participante do referido processo de seleção;
e) à elaboração da proposta é de nossa responsabilidade,
f) não empregamos menores de 18 anos em trabalho noturno, perigoso ou insalubre e nem menores de 16 anos, em qualquer trabalho, salvo na condição de aprendiz a partir de 14 anos, e
g) que concordamos com a Política de Proteção de Dados Pessoais e Privacidade do SESI-SP e do SENAI-SP, disponibilizada nos links: https://privacidade.sesisp.org.br e https://www.sp.senai.br/termos-de-uso-e-politica-de-privacidade

(Local e Data)

_____

(Nome completo e assinatura do representante legal)

ANEXO B

MEMORIAL DESCRITIVO

1. OBJETO

1.1. Contratação de empresa especializada para o fornecimento, treinamento, instalação, configuração e migração de solução de segurança de rede do tipo **Next Generation Firewall (NGFW) e recursos de segurança,** da fabricante Fortinet, para atender às necessidades do SESI-SP e SENAI-SP.

2. JUSTIFICATIVA

2.1. Adoção de uma solução de Firewall de Próxima Geração (NGFW) na sede corporativa do SESI-SP e SENAI-SP é imperativa para assegurar a tríade da segurança da informação: confidencialidade, integridade e disponibilidade. Dada a criticidade dos serviços digitais e o volume de dados institucionais, a infraestrutura exige uma arquitetura robusta, resiliente e alinhada às melhores práticas de mercado (Cybersecurity Mesh Architecture).

2.2. Considerando que a sede concentra serviços essenciais de infraestrutura e a terminação de múltiplos links de internet de 3 Gbps, a solução proposta deve garantir alto throughput e escalabilidade. A arquitetura em Malha Híbrida permitirá a aplicação consistente de políticas de segurança em ambientes on-premises, nuvem e interconexões entre unidades.

2.3. A exigência de operação em Cluster de Alta Disponibilidade (H.A.) justifica-se pela mitigação de riscos de interrupção operacional. A indisponibilidade dos serviços de borda paralisaria atividades administrativas e educacionais, tornando indispensável a redundância de hardware para garantir a resiliência do ambiente.

2.4. A escolha tecnológica recai sobre o fabricante Fortinet visando a integração nativa com o ecossistema de gestão e análise já operante no SESI-SP e SENAI-SP, que inclui:

a) FortiManager: Gestão centralizada para orquestração de políticas e conformidade. Provisionamento “zero touch” e gerenciamento SD-WAN, permitindo facilidade na administração nas políticas de segurança para filiais e controle de redes complexas com monitoria do desempenho e ajustes de links em tempo real. Gerenciador do ambiente, concentrando a gestão dos demais módulos de segurança; e

b) FortiAnalyzer: Central de logs e telemetria para análise correlacionada de eventos. Permite resposta a incidentes de segurança com a visualização em tempo real de ameaças, aplicações em uso e usuários. Geração de relatórios técnicos para gestão executiva e auditorias, em conformidade com a LGPD.

2.5. A manutenção da homogeneidade do parque tecnológico proporciona:

a) Eficiência Operacional: Utilização da *expertise* técnica já consolidada da equipe, reduzindo a curva de aprendizado e riscos de erros de configuração;

b) Interoperabilidade Nativa: Eliminação de conflitos de compatibilidade comuns em ambientes heterogêneos (multivendor);
c) Padronização Operacional: A equipe de TI já possui conhecimento técnico consolidado nas soluções Fortinet, o que reduz a curva de aprendizado, minimiza riscos de erros de configuração e agiliza a resolução de incidentes;
d) Otimização de Custos: Aproveitamento das licenças de gestão existentes e redução de custos com novos treinamentos e plataformas de monitoramento distintas; e
e) Resposta a Incidentes: Agilidade na detecção e remediação de ameaças através da correlação automatizada de logs entre os ativos de rede e segurança.

2.6. A opção pela contratação de subscrições de segurança e suporte com vigência de 5 (cinco) anos, em detrimento do modelo anualizado (1 ano), fundamenta-se nos seguintes aspectos técnicos, econômicos e administrativos:

a) Previsibilidade Orçamentária e Proteção Inflacionária: A aquisição plurianual assegura a imunidade do SESI-SP e SENAI-SP contra reajustes anuais de preços do fabricante, variações cambiais de moedas estrangeiras (visto que o mercado de ativos de segurança é fortemente indexado ao dólar) e reajustes inflacionários do período, fixando o custo de OPEX desde o primeiro dia;
b) Economia de Escala (TCO - Total Cost of Ownership): Os fabricantes aplicam descontos progressivos agressivos em contratos de longo prazo. O custo total de cinco renovações anuais sucessivas supera significativamente o valor de uma única contratação por 5 anos, gerando uma economia real de recursos públicos/institucionais;
c) Eficiência Administrativa e Desburocratização: O ciclo de vida útil estimado para o hardware de segurança de borda é de 5 anos. Optar por licenças anuais exigiria a abertura de novos processos internos de renovação ou termos aditivos a cada 12 meses. A vigência de 5 anos elimina esse esforço burocrático contínuo, otimizando o tempo das equipes de compras, jurídica, TI e de todo pessoal envolvido;
d) Continuidade da Proteção do Ambiente: Dispositivos de borda não podem sofrer descontinuidade no suporte e atualizações de segurança (IPS, Antivirus, Web Filtering) sob o risco de expor toda a rede corporativa. O licenciamento por 5 anos garante a perenidade do suporte técnico do fabricante e a atualização ininterrupta contra ameaças cibernéticas durante todo o ciclo de vida planejado para o hardware, mitigando o risco de "janelas de exposição" por atrasos burocráticos em renovações anuais.

3. DA LOCALIDADE

3.1. O local da prestação do serviço, objeto desse memorial descritivo, ocorrerá em 2 locais distintos, ficando a critério da CONTRATANTE a sua disposição, conforme segue:

3.1.1. SEDE do SESI-SP e SENAI-SP situado na Avenida Paulista, 1313, bela vista, na cidade de São Paulo;
3.1.2. DATACENTER do SESI-SP e SENAI-SP situado na Av. Roberto Pinto Sobrinho, 350 – Vila Menck, Osasco – SP.

4. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

4.1. Das Diretrizes Gerais da Solução:

4.1.1. Equipamentos conforme especificação técnica, configurados em Alta Disponibilidade. A solução deve apresentar capacidades nominais de processamento, inspeção de pacotes e filtragem de conteúdo dimensionadas para a criticidade e o volume de tráfego das entidades atendidas.

4.1.2. Visando a centralização da responsabilidade técnica, a CONTRATADA deverá prover integralmente os equipamentos, o treinamento e a migração, atuando como ponto único de contato (SPOC) para gerenciamento, suporte e interlocução junto ao fabricante.

4.1.3. Os equipamentos deverão ser entregues com subscrição de serviços de segurança e suporte técnico especializado pelo período de 60 (sessenta) meses e incluir as modalidades de proteção avançada IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service.

4.1.4. Deverá ser fornecido 10 unidades de licenças SASE por firewall pelo período de 12 meses, pois será iniciado a alteração de como os nossos usuários acessam a internet e as aplicações internas, e, por isso, faremos de forma controlada, inicialmente, em ambiente de produção controlado, garantindo a compatibilidade técnica com os sistemas legados e validando a latência e configuração dos acessos via SDWAN e cloud security antes da expansão do projeto.

4.1.5. Visando a resiliência da gestão, deverá ser fornecida 01 (uma) licença de FortiManager (instância adicional para redundância local), garantindo a continuidade da orquestração e aplicação de políticas de segurança na Sede na eventualidade de falha de conectividade com o Datacenter principal.

4.1.6. As demais licenças devem ser compreendidas por licenças de suporte prestando maior atenção ao ambiente que deve ser acompanhado de perto por especialistas da solução e, em caso de substituição de peças, deverá ser atendido a troca de forma ágil e priorizada.

4.1.7. É imprescindível que a cobertura das licenças e do serviço FortiCare seja contínua durante todo o período de vigência contratual, garantindo a proteção ininterrupta e o pleno funcionamento da solução de firewall em Alta Disponibilidade.

4.2. Lista de Materiais

ITEM	DESCRIÇÃO	QTD	PARTNUMBER	DESCRIÇÃO
1	FortiGate-201G	2	FG-201G	10 x GE RJ45 (including 1 x MGMT port, 1 x HA port, 8 x switch ports), 4 x GE SFP slots, 8 x 5GE RJ45, 8 x 10GE SFP+ slots, NP7Lite and CP10 hardware accelerated, 480GB onboard SSD storage.

ITEM	DESCRIÇÃO	QTD	PARTNUMBER	DESCRIÇÃO
2	FortiGate-201G UTP License for **5 years**	2	FC-10-F2H1G-950-02-60	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)
3	FW201G SASE 10 user access for **1 Yea**r per FW ***(item correspondente ao reajuste subitem 11.6.1 do Chamamento Público)***	2	FC-10-F2H1G-1329-02-12	SD-WAN Service Bundle (SDWAN Underlay & Application Montioring, FortiGuard SD-WAN SLA Database Updates, SD-WAN Overlay Orchestration Service, FortiSASE 10-user starter kit, SASE Secure Private Access (SPA) Connector, Attack Surface Security Services, FortiTelemetry Cloud, 1-year cloud-based log retention, and FortiCare Premium).
4	NGFW 201G - RMA Next Day for **5 years**	2	FC-10-F2H1G-210-02-60	Next Calendar Day Delivery Priority RMA Service (Requires FortiCare Premium or FortiCare Elite)
5	1GE SFP SX transceiver module	8	FN-TRAN-SX	1 GE SFP transceiver module, short range 500m, LC connector, MMF, 850nm, -20°C to 85°C, for systems with SFP slots
6	10GE SFP+ transceiver module, short range	12	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots
7	FortiManager - VM License (perpétua)	1	FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/Virtual Domains; allows for total of 2 GB/Day of Logs.
8	FortiManager - VM FortiCare Premium Support for **5 years**	1	FC1-10-M3004-248-02-60	FortiCare Premium Support (1 - 10 devices/Virtual Domains)

4.3. A Solução deverá contemplar, no mínimo:

4.3.1. Este equipamento deve ter a função de NGFW (NEXT GENERATION FIREWALL) atuando com o intuito de consolidar todos os enlaces WAN da unidade, tais como links de Internet, MPLS, entre outros, para utilização da engenharia de, provendo ainda de modo integrado conectividade segura, viabilizando assim o acesso local à Internet de modo seguro.
4.3.2. Deve suportar, no mínimo, 25 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
4.3.3. Deve suportar, no mínimo, 8 Gbps de throughput de IPS;
4.3.4. Deve suportar, no mínimo, 5 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware.

4.3.5. Deve suportar, no mínimo, 6 Gbps de throughput de Inspeção SSL;
4.3.6. Suporte a, no mínimo, 10 milhões de sessões simultâneas TCP;
4.3.7. Suporte a, no mínimo, 350 mil novas sessões TCP por segundo;
4.3.8. Estar licenciado para, ou suportar sem o uso de licença, no mínimo 1900 túneis de VPN IPSec Site-to-Site simultâneos
4.3.9. Estar licenciado para, ou suportar sem o uso de licença, no mínimo 15000 túneis de clientes VPN IPSec Client-to-site simultâneos
4.3.10. Deve Suportar, no mínimo, 30 Gbps de throughput VPN IPSec;
4.3.11. Possuir ao menos interfaces 6 GE RJ45
4.3.12. Possuir ao menos interfaces 4 1GE SFP
4.3.13. Possuir ao menos interfaces 6 10GE SFP+
4.3.14. Possuir ao menos interfaces 4 2.5/5 GE RJ45
4.3.15. Deve ser considerado o fornecimento de 4 transceivers SFP LC connector MMF de 1Gb por equipamento. Deve ser considerado o fornecimento de 2 cordões óticos para cada transceiver, de 3 metros, LC/LC.
4.3.16. Deve ser considerado o fornecimento de 6 transceivers SFP+ LC connector MMF de 10 Gb por equipamento. Deve ser considerado o fornecimento de 2 cordões óticos para cada transceiver, de 3 metros, LC/LC.
4.3.17. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
4.3.18. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
4.3.19. Deve possuir unidade do tipo SSD com no mínimo 450 GB para armazenamento de informações locais;
4.3.20. Estar licenciado e ter incluído sem custo adicional, no mínimo, 10 (dez) sistemas virtuais lógicos por equipamento. Entende-se por sistema virtual lógico a possibilidade de dividir um único equipamento físico em várias unidades virtuais, tendo um contexto para WAN e outro contexto para LAN, por exemplo.
4.3.21. Possuir 2 fontes de alimentação de 100–240V AC.
4.3.22. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
4.3.23. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
4.3.24. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em listas de end-of-life e end-of-sale;
4.3.25. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
4.3.26. As funcionalidades de proteção de rede que compõem a solução de segurança, podem funcionar em múltiplos *appliances* desde que atendam a todos os requisitos desta especificação;
4.3.27. Deverá possuir e estar licenciado pelo período de 5 anoscom as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, e Virtualização.

4.3.28. Deve possuir fonte de alimentação AC redundante;

4.4. Funcionalidades

4.4.1. Deve possuir licenciamento durante a vigência do contrato para as subscrições de filtro web e de conteúdo, IPS, controle de aplicação, proteção contra ameaças avançadas incluindo, mas não se limitando a antivírus, botnet, sandbox, entre outras subscrições que façam parte do produto e da oferta.

4.4.2. Deve ser entregue em alta disponibilidade do tipo ativo-passivo com sincronismo de sessão, ou seja, em caso de falha do equipamento primário, o secundário retoma todas as sessões que estavam sendo previamente processadas, evitando assim interrupção no serviço e minimizando o impacto ao referido órgão.

4.4.3. A solução deverá estar devidamente licenciada por 60 meses para atender as funções, funcionalidades e serviços para no mínimo:

4.4.3.1. Controle de Aplicações;
4.4.3.2. Proteção IPS;
4.4.3.3. Proteção contra Ameaças Avançadas;
4.4.3.4. Filtro Web e de Conteúdo;
4.4.3.5. Análise de malwares modernos em nuvem do mesmo fabricante;
4.4.3.6. Roteamento inteligente de aplicações;
4.4.3.7. VPN site-to-site e client-to-site;
4.4.3.8. Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7

4.4.4. A solução deve consistir em plataforma de proteção de rede baseada em equipamento físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source.

4.4.5. Todos os equipamentos a serem fornecidos, bem como seu hardware e software, deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos.

4.4.6. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

4.4.7. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI.

4.4.8. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

4.4.9. Deverá suportar tags de VLAN (802.1Q).

4.4.10. Deverá possuir suporte a agregação de links via 802.3ad LACP.

4.4.11. Deverá possuir ferramenta de diagnóstico do tipo tcpdump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark.

4.4.12. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory.

4.4.13. Deverá possuir integração com tokens para autenticação de duplo fator.

4.4.14. Deverá suportar single-sign-on.

4.4.15. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT.

4.4.16. Deve suportar implementação de Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

4.4.17. Deverá suportar roteamento estático para IPv4 e IPv6.

4.4.18. Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, OSPFv2, OSPFv3, BGP, RIP).

4.4.19. Deverá suportar ECMP.

4.4.20. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).

4.4.21. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay.

4.4.22. Deverá suportar aplicações multimídia, tais como: H.323 e SIP.

4.4.23. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões.

4.4.24. Deverá permitir o funcionamento em modo transparente tipo “bridge”.

4.4.25. Deverá suportar PBR – Policy Based Routing.

4.4.26. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando).

4.4.27. Deverá possuir mecanismo de anti-spoofing.

4.4.28. Deverá permitir criação de regras definidas pelo usuário.

4.4.29. Deverá suportar sFlow ou Netflow.

4.4.30. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.

4.4.31. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS.

4.4.32. Deverá permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.4.33. Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs).

4.4.34. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas.

4.4.35. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual.

4.4.36. Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo.

4.4.37. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e eventos de segurança.

4.4.38. Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais.

4.4.39. Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada.

4.4.40. Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos.

4.4.41. Deverá suportar ambientes multi-cloud.

4.4.42. Deverá possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa.

4.4.43. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo.

4.4.44. A configuração em alta disponibilidade deve sincronizar.

4.4.45. Sessões.

4.4.46. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede.

4.4.47. Associações de Segurança das VPNs.

4.4.48. Tabelas FIB.

4.4.49. Assinaturas de IPS, Antivírus e AntiSpyware.

4.4.50. A configuração de alta disponibilidade deve possibilitar monitoração de falha de link.

4.4.51. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.4.52. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

4.4.53. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

4.4.54. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

4.4.55. Deverá possuir controle de acesso à Internet por endereço IP de origem e destino.

4.4.56. Deverá possuir controle de acesso à Internet por subrede.

4.4.57. Deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC.

4.4.58. Deverá suportar controles por zonas de segurança.

4.4.59. Deverá suportar controles de políticas por porta e protocolo.

4.4.60. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações.

4.4.61. Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança.

4.4.62. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado.

4.4.63. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.4.64. Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado.

4.4.65. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída.

4.4.66. Deve ser possível realizar um espelhamento do tráfego de-criptografado.

4.4.67. Deve de-criptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3.

4.4.68. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de web sites públicos estão utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos.

4.4.69. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada.

4.4.70. Deve suportar objetos e regras de endereço IPv4 e IPv6 consolidados na mesma política de firewall.

4.4.71. Suporte a objetos e regras multicast.

4.4.72. Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego.

4.4.73. Deve possuir indicadores de detecção de vulnerabilidades detectadas de ativos na rede.

4.4.74. Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos.

4.4.75. Deve possuir indicações na interface de sugestões de melhores práticas e avisos de posturas de segurança para serem aplicados no firewall, baseados em controles como CIS 3 e CIS 10, além de sugestões do próprio fabricante.

4.4.76. Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução.

4.4.77. Deve possuir controle de aplicações SaaS como Microsoft Office 365 e G-Suite, a nível de identificar e bloquear acessos a instâncias fora das instâncias da corporação.

4.4.78. Deve possuir base de dados do fabricante para identificação dinâmica de padrões de dados como cartões de crédito e CPF e bloqueio desses dados no firewall.

4.4.79. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.4.80. Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo.

4.4.81. Todos os equipamentos de NGFW, devem estar homologados na ANATEL.

4.4.82. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.

4.4.83. Deve suportar o protocolo padrão da indústria VXLAN.

4.4.84. Enviar log para sistemas de monitoração externos.

4.4.85. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL.

4.4.86. Suportar OSPF graceful restart.

4.4.87. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.

4.4.88. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

4.4.89. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática.

4.4.90. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes.

4.4.91. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos.

4.4.92. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

4.4.93. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2).

4.4.94. Suporte a objetos e regras IPV6.

4.5. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS:

4.5.1. A solução deve ser capaz de agregar vários links em uma interface virtual:

4.5.1.1. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
4.5.1.2. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
4.5.1.3. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
4.5.1.4. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
4.5.1.5. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
4.5.1.6. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
4.5.1.7. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
4.5.1.8. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
4.5.1.9. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
4.5.1.10. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
4.5.1.11. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
4.5.1.12. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
4.5.1.13. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook etc);
4.5.1.14. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações

entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;
4.5.1.15.A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
4.5.1.16.A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
4.5.1.17.A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;
4.5.1.18.A solução deve suportar nativamente conectores com clouds públicas;
4.5.1.19.Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
4.5.1.20.A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
4.5.1.21.Deve implementar balanceamento de link por hash do IP de origem e destino;
4.5.1.22.Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
4.5.1.23.O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

4.6. Funcionalidade de controlador de Rede sem fio

4.6.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

4.6.1.1. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
4.6.1.2. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
4.6.1.3. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
4.6.1.4. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
4.6.1.5. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
4.6.1.6. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

4.6.1.7. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
4.6.1.8. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
4.6.1.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
4.6.1.10.Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
4.6.1.11.Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
4.6.1.12.A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
4.6.1.13.A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
4.6.1.14.A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
4.6.1.15.A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
4.6.1.16.A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
4.6.1.17.A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como *Rogue APs*. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

4.6.1.18.A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
4.6.1.19.A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
4.6.1.20.A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
4.6.1.21.A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
4.6.1.22.A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
4.6.1.23.A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
4.6.1.24.A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
4.6.1.25.Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
4.6.1.26.A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
4.6.1.27.A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
4.6.1.28.A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
4.6.1.29.A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
4.6.1.30.A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
4.6.1.31.A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
4.6.1.32.A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está

conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

4.6.1.33.Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

4.6.1.34.A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

4.6.1.35.A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

4.6.1.36.A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;

4.6.1.37.A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

4.6.1.38.A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

4.6.1.39.A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

4.6.1.40.A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

4.6.1.41.A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

4.6.1.42.A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

4.6.1.43.A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

4.6.1.44.Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

4.6.1.45.Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

4.6.1.46.Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

4.6.1.47.A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

4.6.1.48.Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

4.6.1.49.A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

4.6.1.50.A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

4.6.1.51.A solução deve suportar autenticação 802.1X/EAP, com suporte nativo a EAP-TLS, EAP-TTLS e PEAP, e permitir a utilização de outros métodos EAP por meio de integração com servidores RADIUS/AAA;
4.6.1.52.A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal.
4.6.1.53.A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
4.6.1.54.A solução deve permitir a hospedagem do Captive portal na memória interna do controlador wireless;
4.6.1.55.A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
4.6.1.56.A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
4.6.1.57.A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
4.6.1.58.A solução deve permitir a configuração do Captive portal com endereço IPv6;
4.6.1.59.A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
4.6.1.60.A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
4.6.1.61.Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
4.6.1.62.A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
4.6.1.63.A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
4.6.1.64.A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
4.6.1.65.A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
4.6.1.66.A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
4.6.1.67.A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
4.6.1.68.A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
4.6.1.69.A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
4.6.1.70.A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
4.6.1.71.A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

4.6.1.72.A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
4.6.1.73.A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (EtherLike-MIB);
4.6.1.74.A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato.pcap;
4.6.1.75.A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
4.6.1.76.A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
4.6.1.77.A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
4.6.1.78.A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
4.6.1.79.A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
4.6.1.80.A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
4.6.1.81.A solução deve possuir ferramentas de diagnósticos e debug;
4.6.1.82.A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
4.6.1.83.A solução deve suportar comunicação com elementos externos através de REST API;
4.6.1.84.A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;
4.6.1.85.Deve estar licenciado para gerenciar no mínimo 100 pontos de acesso sem fio em modo tunnel.

4.7. Funcionalidade de controlador de Rede Cabeada

4.7.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
4.7.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
4.7.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
4.7.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
4.7.5. Deve montar a topologia da rede de maneira automática;
4.7.6. Deve ser capaz de configurar os switches da rede;
4.7.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

4.7.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
4.7.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
4.7.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
4.7.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
4.7.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
4.7.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
4.7.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
4.7.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
4.7.16. Deve ser capaz de configurar parâmetros SNMP dos switches;
4.7.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
4.7.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
4.7.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
4.7.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
4.7.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
4.7.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
4.7.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
4.7.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;
4.7.25. Deve estar licenciado para gerenciar no mínimo 50 switches simultaneamente em um único appliance;

4.8. Funcionalidades de controle de aplicações:

4.8.1. Deverá reconhecer, no mínimo, 4500 (quatro mil e quinhentas) aplicações com base na camada 7 do modelo OSI;
4.8.2. Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários;
4.8.3. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
4.8.4. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.8.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
4.8.6. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.8.7. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante;
4.8.8. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.8.9. Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação.
4.8.10. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
4.8.11. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
4.8.12. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
4.8.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
4.8.14. Deverá atualizar a base de assinaturas de aplicações automaticamente;
4.8.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
4.8.16. Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação;
4.8.17. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
4.8.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.) possuindo granularidade de controle/políticas para os mesmos;
4.8.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
4.8.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate etc) possuindo granularidade de controle/políticas para os mesmos;
4.8.21. Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
4.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação e Categoria da aplicação;
4.8.23. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet.
4.8.24. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP.
4.8.25. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
4.8.26. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-

proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

4.8.27. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.8.28. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.8.29. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.8.30. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

4.8.31. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.8.32. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

4.8.33. Deve alertar o usuário quando uma aplicação for bloqueada;

4.8.34. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol etc);

4.8.35. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

4.8.36. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.8.37. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

4.9. Funcionalidades de IPS

4.9.1. Deverá permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

4.9.2. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

4.9.3. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.9.4. Deverá possuir integração à plataforma de segurança;

4.9.5. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

4.9.6. Deverá utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas.

4.9.7. Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego.

4.9.8. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego;
4.9.9. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
4.9.10. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc;
4.9.11. Detectar e bloquear a origem de portscans;
4.9.12. Bloquear ataques efetuados por worms conhecidos;
4.9.13. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
4.9.14. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.9.15. Implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo;
4.9.16. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.9.17. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP e POP3;
4.9.18. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento;
4.9.19. Deve permitir o bloqueio de vulnerabilidades;
4.9.20. Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos;
4.9.21. Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos.
4.9.22. Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros.
4.9.23. Deve ser possível escanear e bloquear conexões a servidores de botnet.
4.9.24. Deve dispor de opção para bloquear URLs maliciosas mediante base de dados local.
4.9.25. Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS.
4.9.26. Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS.
4.9.27. Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros.
4.9.28. Deve ser possível filtrar assinaturas com base no identificador CVE.
4.9.29. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um “wildcard” do CVE para abranger mais de um identificador;
4.9.30. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável.
4.9.31. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
4.9.32. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.9.33. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
4.9.34. Os eventos devem identificar o país de onde partiu a ameaça;
4.9.35. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
4.9.36. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
4.9.37. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
4.9.38. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante.
4.9.39. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
4.9.40. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
4.9.41. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;
4.9.42. Deve permitir o bloqueio de exploits conhecidos.

4.10. Funcionalidades de Proteção Contra Ameaças Avançadas

4.10.1. Deverá possuir funções de antivírus e anti-spyware;
4.10.2. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
4.10.3. Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros);
4.10.4. Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas.
4.10.5. Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
4.10.6. Deverá permitir o bloqueio de download de arquivos por tamanho;
4.10.7. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
4.10.8. Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros.

4.10.9. Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos.
4.10.10. A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque;
4.10.11. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
4.10.12. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back;
4.10.13. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;
4.10.14. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.11. Funcionalidades de Filtro Web E Conteúdo

4.11.1. Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.11.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
4.11.3. Deverá possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
4.11.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;
4.11.5. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4.11.6. Deverá possuir a função de exclusão de URLs do bloqueio;
4.11.7. Deverá permitir a customização de página de bloqueio;
4.11.8. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
4.11.9. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário.
4.11.10. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego.
4.11.11. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website.
4.11.12. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;
4.11.13. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.11.14. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
4.11.15. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
4.11.16. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4.11.17. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
4.11.18. Possuir pelo menos 80 (oitenta) categorias de URLs;
4.11.19. Deve possuir a função de exclusão de URLs do bloqueio;
4.11.20. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
4.11.21. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
4.11.22. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

4.12. Identificação dos Usuários

4.12.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
4.12.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
4.12.3. Deve possuir integração e suporte a Microsoft Active Directory para, no mínimo, o sistema operacional Windows Server 2012 R2;
4.12.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando SSO (Single Sign-On). Essa funcionalidade não deve possuir limites quanto a licenciamento de usuários;
4.12.5. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
4.12.6. Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
4.12.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a Internet para que antes de iniciar a navegação, apresente-se um portal de autenticação residente no firewall do tipo portal cativo;
4.12.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix, VMware Horizon e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.12.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
4.12.10. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

4.13. Funcionalidades de VPN

4.13.1. Suportar VPN Site-to-Site e Client-to-Site;
4.13.2. Suportar IPSec VPN;
4.13.3. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
4.13.4. A VPN IPSec deverá suportar AES 256 (Advanced Encryption Standard);
4.13.5. A VPN IPSec deverá suportar autenticação MD5, SHA384 e SHA512;
4.13.6. A VPN IPSec deverá suportar Diffie-Hellman Grupos 27 a 32;
4.13.7. A VPN IPSec deve suportar algoritmo Internet Key Exchange (IKE v1 e v2);
4.13.8. Deverá permitir habilitar e desabilitar túneis de VPN IPSec a partir da interface gráfica da solução, facilitando o processo de resolução de problemas;
4.13.9. A VPN IPSec deve suportar Forward Error Correction (FEC);
4.13.10. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
4.13.11. Solução deverá ser capaz de prover uma arquitetura similar ao conceito de Auto Discovery VPN – ADVPN;
4.13.12. Deve suportar NAT Traversal;
4.13.13. A VPN IPSec deve ser compatível com ambiente em alta disponibilidade garantindo que o tráfego de VPN não sofrerá interrupção durante um evento de HA.
4.13.14. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL.
4.13.15. O agente de VPN IPSec client-to-site, o qual deve ser do mesmo fabricante do Firewall, deve ser compatível com pelo menos: Windows 10 (64 bit), Windows 11 (64 bit), Mac OS X (v13 ou superior), Ubuntu 22 ou superior, RedHat 9 ou superior, CentOS Stream 9 ou superior.
4.13.16. Deve ser possível realizar algumas verificações da estação do usuário durante a conexão de VPN, tais como verificações de sistema operacional, antivírus habilitado, firewall habilitado, processo rodando e validação de chave de registro.
4.13.17. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
4.13.18. A VPN IPSEc deve suportar Diffie-Hellman Group1, Group2, Group5, Group 14;
4.13.19. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
4.13.20. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;
4.13.21. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
4.13.22. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
4.13.23. Atribuição de DNS nos clientes remotos de VPN;
4.13.24. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN;
4.13.25. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
4.13.26. Suportar leitura e verificação de CRL (Certificate Revocation List);

4.13.27. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis VPN;
4.13.28. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
4.13.29. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
4.13.30. Deverá manter uma conexão segura com o portal durante a sessão;

4.14. Funcionalidades de roteamento Inteligente de Aplicação

4.14.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
4.14.2. Deverá ser capaz de agregar pelo menos 03 (três) links em uma interface virtual;
4.14.3. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de verificações de saúde dos links WAN, permitindo testes de resposta por PING, HTTP, TCP/UDP ECHO e DNS. Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
4.14.4. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
4.14.5. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
4.14.6. Deve suportar o uso de VRF (Virtual Routing and Forwarding) e Multi-VRF;
4.14.7. A solução de deve possuir suporte a Policy Based Routing ou Policy Based Forwarding;
4.14.8. Deve suportar roteamento estático e dinâmico (OSPFv2/v3, BGPv4/BGP4+, RIPv2);
4.14.9. Deverá poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNs);
4.14.10. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
4.14.11. Deverá permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da interface virtual;
4.14.12. Deve desempenhar a função de duplicidade de pacote permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não ocorrer retransmissão;
4.14.13. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
4.14.14. Deve permitir configurar o código de DiffServ (DSCP) do pacote ESP do túnel IPSec;
4.14.15. Deverá permitir marcar com DSCP os testes de link para obter uma avaliação mais realista da qualidade de um determinado link;
4.14.16. Deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em:
4.14.17. Número de Sessões,
4.14.18. Volume de Tráfego,
4.14.19. IP de Origem e Destino;
4.14.20. Transbordo de Link baseado em limite de banda.
4.14.21. As regras de escolha de roteamento devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de origem e destino e serviços de Internet.

4.14.22. Deve permitir a customização dos tempos para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido.
4.14.23. A solução de deve prover estatísticas em tempo real na interface web a respeito da ocupação de banda (upload e download) e desempenho das verificações de saúde (perda de pacote, jitter e latência);
4.14.24. Deve ser possível configurar a porcentagem de perda de pacote e o tempo de latência e jitter na verificação de estado de saúde do link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
4.14.25. Deve dispor de opção que maximize o uso da largura de banda utilizando os links WANs que estejam dentro do nível de saúde estipulado.
4.14.26. Deve ser possível monitorar a saúde do link de modo passivo, sem a emissão de pacotes de verificação, utilizando somente informações das sessões que transitam pelo equipamento.
4.14.27. Deve ser possível utilizar o método de verificação de saúde passivo na existência de tráfego e ativo na inexistência de tráfego.
4.14.28. Deve suportar balanceamento de tráfego por sessão e pacote;
4.14.29. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

4.15. QUALITY OF SERVICE

4.15.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, BitTorrent etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de largura de banda máxima quando forem solicitadas por diferentes usuários ou aplicações.
4.15.2. Deve suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
4.15.3. por endereço de origem;
4.15.4. por endereço de destino;
4.15.5. por usuário e grupo;
4.15.6. por aplicações;
4.15.7. por protocolo e porta;
4.15.8. por categoria de URL;
4.15.9. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
4.15.10. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
4.15.11. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
4.15.12. O QoS deve possibilitar a definição de fila de prioridade;
4.15.13. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o vínculo com categorias de URL, IPs de origem e destino, grupos de usuários, protocolos e portas;

4.15.14. Deve ter a capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas e mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
4.15.15. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que tiverem correspondência na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que tiverem correspondência na regra;
4.15.16. Deve possibilitar a definição de bandas distintas para download e upload;
4.15.17. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
4.15.18. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
4.15.19. Endereço de origem;
4.15.20. Endereço de destino;
4.15.21. Usuário e grupo;
4.15.22. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
4.15.23. Por porta;
4.15.24. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
4.15.25. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
4.15.26. Suportar modificação de valores DSCP para o Diffserv;
4.15.27. Suportar priorização de tráfego usando informação de ToS (Type of Service);
4.15.28. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
4.15.29. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

4.16. Funcionalidade de Filtro de Dados

4.16.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
4.16.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.16.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.16.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.
4.16.5. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

4.17. Solução de Gerenciamento Centralizado

4.17.1. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da CONTRATANTE a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

4.17.2. Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;
4.17.3. Poderá ser entregue em formato de appliance físico ou appliance virtual;
4.17.4. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012/2016/2019, KVM no Redhat 7.1, Nutanix AHV (AOS 5.10.5);
4.17.5. Deverá ser compatível com ambientes em nuvem, tais como AWS, GCP, OCI e Azure.
4.17.6. A solução deverá estar devidamente licenciada para:
4.17.7. Gerenciar, no mínimo, 10 unidades (appliances e sistemas virtuais) dos equipamentos da solução de SD-WAN de forma simultânea;
4.17.8. Para máquina virtual os itens abaixo devem ser atendidos:
4.17.9. Não deverá existir limite para o número de vCPUs alocadas no appliance virtual;
4.17.10. Não deverá existir limite para a expansão da memória RAM no appliance virtual;
4.17.11. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
4.17.12. Deve suportar VMware vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
4.17.13. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
4.17.14. A solução deve suportar o uso de APIs para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
4.17.15. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
4.17.16. Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;
4.17.17. Deve ser possível criar grupos de dispositivos, tais como appliances do Data Center e appliances dos Sites Remotos para vínculo de políticas diferentes.
4.17.18. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
4.17.19. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.
4.17.20. Possibilitar a criação e administração de políticas de firewall, controle de aplicação e SD-WAN;
4.17.21. Deve ser possível visualizar quem criou e quem modificou uma determinada política de firewall, especificando ainda a data e horário.
4.17.22. Deve ser possível criar modelos de configurações de BGP, SD-WAN, IPSec, CLI e até mesmo configurações globais do sistema visando associar a um grupo de dispositivos.
4.17.23. A solução deve disponibilizar um modelo de configuração recomendado para BGP e IPSec visando auxiliar na configuração de uma topologia SD-WAN hub and spoke.
4.17.24. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
4.17.25. Deve ser possível filtrar no gráfico de monitoramento de SD-WAN por dispositivos e interfaces não saudáveis.

4.17.26. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
4.17.27. A solução central deve atuar como autoridade certificadora visando assinar certificados emitidos para os appliances de SD-WAN e estabelecer túneis IPSec por meio destes certificados, proporcionando mais segurança ao ambiente.
4.17.28. Permitir usar palavras chaves ou cores para facilitar identificação de regras;
4.17.29. Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;
4.17.30. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
4.17.31. Permitir criação de regras que fiquem ativas em horário definido;
4.17.32. Permitir criação de regras com data de expiração;
4.17.33. Deve ser possível trabalhar com variáveis visando manipular políticas associadas com essas variáveis, tal como identificador único de cada localidade.
4.17.34. Realizar o backup das configurações para permitir o retorno de uma configuração salva;
4.17.35. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
4.17.36. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
4.17.37. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
4.17.38. Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;
4.17.39. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
4.17.40. Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
4.17.41. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, SAML, TACACS+ e PKI.
4.17.42. Deve suportar segundo fator de autenticação para os administradores da solução.
4.17.43. Deve suportar integração com soluções de ITSM para abertura de chamados, a citar, por exemplo, integração com ServiceNow.
4.17.44. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;
4.17.45. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
4.17.46. Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);
4.17.47. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
4.17.48. Gerar alertas automáticos via Email, SNMP e Syslog;
4.17.49. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

4.17.50. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.
4.17.51. Permitir backup das configurações e rollback de configuração para a última configuração salva;

4.18. SERVIÇO DE ACESSO SEGURO DE BORDA (SASE)

4.18.1. Características Gerais

4.18.1.1. A gerência deve ser disponibilizada em nuvem, sem usar qualquer recurso local;
4.18.1.2. A solução SASE deve ser baseada em uma arquitetura em nuvem, permitindo a integração de funções de rede e segurança como serviço em uma única plataforma;
4.18.1.3. O acesso a console de administração da solução SASE deve ser feito via navegador web e ter a possibilidade de se integrar com IdP para autenticação SSO dos usuários administrativos;
4.18.1.4. A solução SASE deve garantir o acesso seguro à web, serviços em nuvem e aplicações privadas, independentemente da localização do usuário ou de onde essas aplicações estão hospedadas;
4.18.1.5. A solução SASE deve ser (SaaS) software baseado em serviço que permite aos clientes acessarem a Internet com segurança e proteção. Deve garantir a proteção de endpoints e usuários remotos off-net (fora da rede) com o mesmo nível de segurança de quando estão na rede, independentemente de sua localização;
4.18.1.6. A solução SASE deve ser composta por, no mínimo:
4.18.1.7. FWaaS (Firewall as a Service);
4.18.1.8. SWG (Secure Web Gateway);
4.18.1.9. CASB (Cloud Access Security Broker);
4.18.1.10. ZTNA (Zero Trust Network Access);
4.18.1.11. SD-WAN (Software-Defined Wide-Area Network);
4.18.1.12. DLP (Data Loss Prevention);
4.18.1.13. Todos os componentes da solução SASE devem ser de um único fabricante, ou seja, deve ser uma solução Single-Vendor SASE (conforme definição cunhada pelo Gartner);
4.18.1.14. A solução SASE deve ter cobertura mundial, com possibilidade de provisionamento nos seguintes continentes: Américas, Europa, África, Ásia e Oceania;
4.18.1.15. A solução SASE deve permitir e estar licenciado para provisionamento em, no mínimo, 4 (quatro) pontos de presença (POP).
4.18.1.16. Ao menos um ponto de presença deve estar disponível obrigatoriamente no Brasil;
4.18.1.17. Os 4 (quatro) pontos de presença incluídos na solução SASE devem permitir a configuração de, no mínimo, 1 (um) endereço de IP fixo para cada. Caso a solução exija licenciamento adicional, este deve ser entregue para todos os POPs;
4.18.1.18. A solução SASE deve possuir, além da redundância geográfica, a possibilidade de o usuário escolher em qual POP os logs serão armazenados para estar em compliance com legislações locais;

4.18.1.19. A plataforma em nuvem da solução SASE deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com disponibilidade mensal de 99,999% para todos os serviços.
4.18.1.20. A solução SASE deverá possuir certificações reconhecidas de segurança e conformidade, tais como SOC 2 e/ou ISO 27001, ISO 27017 e ISO 27018;
4.18.1.21. Quando um tráfego for direcionado a um POP da solução SASE, todo o processamento das funcionalidades de segurança deve acontecer dentro desse mesmo POP, sem que o tráfego seja direcionado para processamento, em cadeia, em diferentes datacenters.
4.18.1.22. A comunicação entre agentes (clientes) e outras soluções de infraestrutura SASE devem sempre usar comunicação segura criptografada.
4.18.1.23. A solução SASE deve permitir a integração com ambiente corporativo, escritórios, sites remotos através de SD-WAN Seguro.
4.18.1.24. A solução SASE deve suportar os acessos:
4.18.1.25. Acesso seguro à Internet (SIA) - com ou sem Agente;
4.18.1.26. Acesso Privado Seguro (SPA) – integração com outras arquiteturas que permitam o acesso privado seguro através de soluções como ZTNA, SD-WAN e NGFW para garantir eficiência e conectividade aos recursos locais sendo que as integrações com soluções NGFW devem ser feitas por comunicação criptografada e preferencialmente por túneis IPSec;
4.18.1.27. Acesso seguro a aplicações SaaS - Através da integração de API com provedores de nuvem, CASB deve adicionar controle e visibilidade aos dados e aplicações sancionados;
4.18.1.28. A solução SASE deve permitir o acesso remoto seguro às aplicações hospedadas localmente (on-Premisse) através da integração de uma arquitetura SASE e ZTNA;
4.18.1.29. A solução SASE deve permitir acesso seguro para aplicações em nuvem com CASB, adicionando mais controle, visibilidade das aplicações permitidas e dados de tráfego através de uma integração com a API do provedor;
4.18.1.30. A solução SASE em conjunto com a arquitetura ZTNA deve permitir controle e análise profunda de postura do endpoint, permitindo o acesso apenas a partir de dispositivos seguros e as características específicas de cada acesso.
4.18.1.31. A solução SASE, deve ter componente de Web Gateway Seguro com base de informações, inteligência, pesquisa e desenvolvimento de proteções com suporte a:
4.18.1.32. Inspeção SSL;
4.18.1.33. Antivírus;
4.18.1.34. IPS;
4.18.1.35. Filtro Web baseado em categorias;
4.18.1.36. Proteção contra domínios de C&C;
4.18.1.37. Inline CASB
4.18.1.38. Filtro de canais de Youtube;
4.18.1.39. A solução SASE deve permitir o redirecionamento do tráfego web para uma solução de isolamento remoto de navegador (RBI), a partir de políticas de segurança que leve em consideração parâmetros tais como a categoria do site visitado e o usuário ou o seu grupo;
4.18.1.40. Caso a solução SASE não possua nativamente uma solução de isolamento remoto de navegador (RBI), o licenciamento de uma solução do mesmo fabricante será

permitido, desde que inclua o quantitativo de licenças para atender todos os clientes da solução SASE;

4.18.1.41. O componente de isolamento remoto de navegador (RBI) deve possuir controle granular para bloquear ou permitir: clicar com o botão direito; imprimir para PDF; fazer o upload e/ou download de arquivos executáveis, de imagem, de texto e do Microsoft Office; copiar e colar textos.

4.18.1.42. Para acessos no formato SWG, sem cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, Radius ou SAML.

4.18.1.43. A solução SASE deve reconhecer o tráfego de rede gerado por um grande número de aplicações. O controle de aplicação com Inline-CASB deve usar decodificadores de protocolo que podem analisar o tráfego de rede para detectar o tráfego de aplicação, mesmo que o tráfego use portas ou protocolos não padrão. O Controle de Aplicação com Inline-CASB deve suportar a detecção de tráfego usando o protocolo HTTP (versões 1.0, 1.1 e 2.0).

4.18.1.44. A solução SASE deve permitir a configuração e adição do Inline-CASB sob demanda, suportar o controle de aplicações SaaS através de inclusão de headers http e restrição de tenant tanto no uso com cliente quanto no uso sem cliente.

4.18.1.45. A solução SASE deve suportar e estar licenciada para controlar, no mínimo, as seguintes aplicações SaaS:

4.18.1.46. Microsoft Office 365;

4.18.1.47. Microsoft OneDrive;

4.18.1.48. Microsoft Teams;

4.18.1.49. Outlook ou Hotmail;

4.18.1.50. ChatGPT;

4.18.1.51. Gmail;

4.18.1.52. Google Workspace (Calendar, Docs, Drive, Meet);

4.18.1.53. Meta (Facebook, Instagram);

4.18.1.54. YouTube;

4.18.1.55. DocuSign;

4.18.1.56. GitHub;

4.18.1.57. LinkedIn;

4.18.1.58. Zoom;

4.18.1.59. A solução SASE deve permitir a geração de relatórios e visualização de logs. Os relatórios e logs deverão informar sobre atividades de rede, detecção de vírus, visita a sites inválidos, intrusões, tentativas de falha de login etc.

4.18.1.60. A solução SASE deve permitir gerar relatórios de dados a partir de logs. Deve permitir executar regularmente relatórios em intervalos programados e executar relatórios manualmente quando desejado.

4.18.1.61. A solução SASE deve possuir módulo de logs para informações estatísticas e de segurança.

4.18.1.62. A solução SASE deve permitir o encaminhamento de forma segura de logs para um servidor externo no formato Syslog ou CEF.

4.18.1.63. Para acessos através de cliente, a solução SASE deve possuir suporte para autenticação de usuários em diretório centralizado através de LDAP, RADIUS ou SAML.

4.18.1.64. A solução SASE deve gerar certificados que serão utilizados pelos Agentes para registro. Apenas certificados gerados pela solução deverão ser aceitos para validação.
4.18.1.65. A solução SASE deve utilizar apenas 01 (um) Agente (Cliente) para a comunicação com a plataforma SASE, ZTNA e outros benefícios como Sandbox, AntiMalware, Varredura de Vulnerabilidades, Inventário de Software, Filtro Web, entre outros.
4.18.1.66. A solução SASE deve permitir que sejam aplicadas políticas de segurança de forma granular para o acesso seguro à Internet e para o acesso a aplicações internas em conjunto com o ZTNA ou Acesso Privado Seguro (SPA), com controle baseado em IP, Aplicação, Usuário ou Grupo de Usuários.
4.18.1.67. O Agente da solução SASE deve ser compatível com os seguintes Sistemas Operacionais: Windows, macOS, Linux, Android e iOS;
4.18.1.68. A solução SASE deve ter integração através do SAML com IdP's como Azure AD e Okta, facilitando a autenticação dos usuários para se conectarem ao ambiente SASE;
4.18.1.69. O Agente da solução SASE deve ser implementado manualmente através do download e inclusão do "Código de Convite" para ativar as funcionalidades;
4.18.1.70. Após o registro do Agente na solução SASE, deve ser possível usar diferentes usuários (um de cada vez) para estabelecer o túnel e enviar tráfego para o SASE;
4.18.1.71. A solução SASE deve possuir o suporte à configuração de uma conexão sempre ativa. A configuração sempre ativa é opcional e customizada pelo administrador da solução.
4.18.1.72. A solução SASE deve suportar a configuração do Acesso à Rede de Confiança Zero (ZTNA) sem instalação de Agente adicional (agentless ZTNA)
4.18.1.73. O acesso a aplicações via ZTNA sem agente deve suportar a configuração de aplicações privadas, que serão roteadas através do recurso Acesso Privado Seguro (SPA);
4.18.1.74. A solução SASE deve ter disponibilidade de pelo menos 0,5 Mbps de tráfego por usuário.
4.18.1.75. A solução SASE deve permitir o controle de mídias removíveis USB nos dispositivos finais.
4.18.1.76. A solução SASE deve permitir o acesso de aplicações privadas através de Proxy ZTNA em um NGFW;
4.18.1.77. O cliente deve possuir funcionalidades de antivírus e envio de arquivos para análise de sandbox para proteção da estação caso o acesso à internet deixe de ser realizado de forma segura via SASE.
4.18.1.78. A solução SASE deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso, impedindo que um cliente não conforme possa se conectar à recursos.
4.18.1.79. A postura deve ser monitorada continuamente para que, caso ocorra alguma alteração de conformidade, o acesso aos recursos possa ser bloqueado.
4.18.1.80. A solução SASE deve permitir a desativação ou ativação da análise de postura dos endpoints.
4.18.1.81. Quando necessária a autenticação WEB para a solução SASE, as informações de login devem ser transmitidas por SSL e mantidas de forma segura.
4.18.1.82. A solução de SASE deve ter console com módulos:
4.18.1.83. Painéis de monitoramento

4.18.1.84. Configurações de Rede
4.18.1.85. Configurações SASE
4.18.1.86. Configurações do Sistema
4.18.1.87. Analytics que pode ser usado para análise em tempo real e elaboração de relatórios
4.18.1.88. A solução de SASE deve permitir criar e modificar o Dashboard (painel web) com matriz personalizável de widgets.
4.18.1.89. A solução SASE deve incluir Dashboards (painéis) para monitorar o inventário de dispositivos, ameaças de segurança, tráfego e saúde da rede. Deve incluir os seguintes painéis:
4.18.1.90. Status: Fornece uma visão geral do seu ambiente SASE atual e do status do endpoint.
4.18.1.91. Mapa de Ativos: Exibe a localização geográfica dos ativos, incluindo servidores, em um mapa global. Também indica qual servidor tem o registro ativado.
4.18.1.92. Visão Única: Sistema abrangente de monitoramento para sua rede que integra dados em tempo real e históricos em uma única visualização. Deve permitir usá-lo para registrar e monitorar ameaças às redes, filtrar dados em vários níveis e acompanhar a atividade administrativa.
4.18.1.93. A solução SASE deve disponibilizar os seguintes monitores:
4.18.1.94. Fontes: Exibe fontes por volume de tráfego e detalhamento por fonte.
4.18.1.95. Thin-Edge: Exibe dispositivos Thin-Edge por volume de tráfego e detalhamento por dispositivo.
4.18.1.96. Destinos: Exibe destinos por volume de tráfego e detalhamento por destino.
4.18.1.97. Aplicações: Exibe aplicações por volume de tráfego e detalhamento por aplicação
4.18.1.98. Aplicações em Nuvem: Exibe aplicações em nuvem e detalhamento por aplicação.
4.18.1.99. Sites da Web: Exibe sites por contagem de sessão e detalhamento por domínio.
4.18.1.100. Políticas: Exibe políticas por volume de tráfego e detalhamento por número de política.
4.18.1.101. Sessões: Exibe sessões por fonte de tráfego.
4.18.1.102. VPN: Exibe conexões VPN por usuário.
4.18.1.103. Ameaças: Exibe ameaças e detalhamento por ameaça.
4.18.1.104. A solução SASE deve permitir visualizar os endpoints gerenciados através do widget de status correspondente ou do monitor de status. Tanto o widget quanto o monitor devem exibir gráficos que mostram informações do endpoint, incluindo o status e a plataforma. Deve permitir o cancelamento do registro de um endpoint a partir do widget ou monitor.
4.18.1.105. Para auxiliar os administradores no diagnóstico de problemas de conectividade e de performance de rede dos usuários remotos, a solução SASE deve incluir recursos de monitoramento fim-a-fim, desde o cliente da solução, passando pelo POP e até as aplicações de destino.
4.18.1.106. A solução SASE deve permitir que monitoramentos sejam executados em tempo real e exibam as informações de consumo de CPU, memória e disco da estação cliente, além dos dados de performance de acesso (perda de pacotes e tempo de ida-volta (RTT)) à aplicação SaaS escolhida.

4.18.1.107. A solução SASE deve permitir perfis administrativos específicos para administradores de leitura ou escrita.
4.18.1.108. A solução SASE deve ter gerenciamento de implantação pela console da solução. Assim, implantações e atualizações de quaisquer soluções complementares podem ser obtidas através da nuvem.
4.18.1.109. A solução SASE deve possuir suporte a segurança e filtros de DNS para os acessos via agente de forma a impedir ataques e acessos inseguros na camada de DNS.
4.18.1.110. A solução SASE deve ter componente FWaaS (Firewall como Serviço) para aplicar políticas com Perfis que incluem Filtro Web, Antimalware, DLP, Filtro DNS, Filtro de Arquivos, IPS, Controle de APP e Inspeção SSL.
4.18.1.111. A solução SASE deve ter mecanismo de prevenção de vazamento de dados para impedir que dados sensíveis saiam e entrem nos dispositivos protegidos.
4.18.1.112. A solução SASE deve trazer dicionários de informações sensíveis, pré-definidos e atualizados automaticamente pelo fabricante, contendo no mínimo: informações financeiras, dados pessoais e códigos fonte), bem como permitir a criação e customização de padrões adicionais conforme necessidade;
4.18.1.113. A solução SASE deve permitir a criação de dicionários personalizados de informações sensíveis, utilizando palavras chaves, expressões regulares e lógica booleana;
4.18.1.114. A solução de SASE deve permitir a personalização de páginas HTML de bloqueio que são exibidas nos endpoints em certas situações com base nas configurações do Controle de Aplicação.
4.18.1.115. A solução SASE deve permitir o login de usuários e aplicar políticas IAM para controle do acesso administrativo.
4.18.1.116. A solução SASE deve implementar MFA para autenticação de usuários administrativos
4.18.1.117. A solução SASE deve manter em sua plataforma em nuvem as regras de segurança, seja para acesso à plataforma ou as políticas impostas pelo SASE, para controlar os usuários remotos. A plataforma de gerenciamento e configuração de políticas de segurança não deve ficar restrita a apenas um PoP e deve ser altamente disponível, replicando os perfis de segurança para todos os PoPs de segurança do cliente.
4.18.1.118. A solução SASE deve inspecionar a camada SSL/TLS durante a inspeção de certificados e as camadas superiores durante a inspeção profunda. A solução SASE deve filtrar e proteger o tráfego seguro que os vários perfis de segurança processaram. A inspeção SSL deve proteger, além do tráfego HTTPS, outros protocolos criptografados comumente usados, como SMTPS, POP3S, IMAPS e FTPS.
4.18.1.119. A configuração do Secure Web Gateway da solução SASE deve ser feita sem a necessidade de um agente no endpoint para acesso HTTP e HTTPS, permitindo que políticas de segurança sejam aplicadas para proteger o acesso.
4.18.1.120. O controle do CASB pode ou não ser efetuado em console separada permitindo maior controle e segmentação de acesso através de perfis de IAM.
4.18.1.121. O módulo CASB deve ter visibilidade de conteúdo do S3 Bucket da AWS, Storage do Azure e GCP, além das integrações do Microsoft e Google Workspace.
4.18.1.122. Cada usuário deve ter direito de uso da solução em no mínimo 3 (três) dispositivos simultâneos.

5. DA PRESTAÇÃO DE SERVIÇO PELA EMPRESA CONTRATADA

5.1. A CONTRATADA deverá prestar os serviços de forma integral, contínua e técnica, garantindo a entrega da solução em total conformidade com as especificações, prazos e Níveis de Serviço (SLAs) estabelecidos neste Memorial Descritivo.

5.2. A prestação dos serviços compreende, obrigatoriamente, as seguintes etapas e atividades:

5.2.1. Elaboração de Plano de Trabalho e Cronograma Detalhado, incluindo o levantamento da topologia lógica e física, validação do ambiente atual e análise de riscos para a estratégia de implementação a ser apresentado pela CONTRATADA no prazo de até 05 (cinco) dias úteis após a assinatura do contrato, como condição para o início da implantação da solução.
5.2.2. Entrega física e conferência integral de hardware, software, licenças e acessórios previstos neste Memorial Descritivo, responsabilizando-se pela integridade dos itens até o aceite parcial.
5.2.3. Montagem dos equipamentos em rack designado, incluindo cabeamento estruturado (identificado e organizado), certificação de conectividade e alimentação elétrica.
5.2.4. Implementação da arquitetura em HA, com sincronização de sessões, parametrização de interfaces e hardening do sistema operacional.
5.2.5. Configuração e integração do FortiManager, incluindo a licença adicional de redundância na Sede, de modo a assegurar continuidade operacional em caso de indisponibilidade de comunicação com o Datacenter;
5.2.6. Migração e importação das regras do firewall atual, com análise prévia da política vigente, mapeamento de objetos, revisão de compatibilidades e execução controlada da transição para a nova plataforma;
5.2.7. Validação das regras migradas, com testes funcionais e verificação de impacto nos serviços críticos, a fim de garantir a preservação da segurança e da disponibilidade do ambiente;
5.2.8. Integração com os recursos de monitoramento e gestão já existentes no ambiente do CONTRATANTE, inclusive com FortiAnalyzer, quando aplicável;
5.2.9. Execução de testes de funcionamento, desempenho e failover, comprovando a correta operação da arquitetura em alta disponibilidade;
5.2.10. Operação assistida, após a implantação, pelo período necessário à estabilização da solução, com acompanhamento técnico e correção de ajustes finos;
5.2.11. Treinamento operacional para a equipe técnica designada pelo CONTRATANTE, contemplando administração, monitoração, procedimentos de contingência e boas práticas de operação;
5.2.12. Fornecimento da documentação técnica final, contendo topologia, parâmetros aplicados, inventário da solução, regras migradas, orientações operacionais e demais informações relevantes para a continuidade da gestão;
5.2.13. Prestação de suporte técnico e garantia, respeitando os prazos de atendimento e resolução previstos neste Memorial;
5.2.14. Atendimento às solicitações do CONTRATANTE em dias úteis, finais de semana e feriados, quando necessário, mediante prévio aviso de 24 (vinte e quatro) horas, sem prejuízo da continuidade operacional;

5.2.15. Observância integral das normas de confidencialidade, segurança da informação e LGPD, responsabilizando-se pela proteção dos dados e informações a que tiver acesso durante toda a execução contratual.

5.2.16. A CONTRATADA deverá manter equipe técnica qualificada, devidamente certificada na solução e com experiência comprovada em soluções Fortinet e em migração de ambientes críticos, capacidade de resposta compatível com a criticidade do ambiente e postura proativa na identificação e correção de eventuais inconsistências durante a implantação.

5.3. Todos os serviços deverão ser executados de forma coordenada, com mínima intervenção no ambiente produtivo e com priorização da continuidade dos serviços essenciais do CONTRATANTE.

5.4. Após a conclusão da migração e entrada em produção, a CONTRATADA deverá realizar a Operação Assistida presencial pelo prazo mínimo de 10 (dez) dias úteis. A permanência do profissional e a conclusão desta etapa observarão as seguintes condições:

5.4.1. O período deve ser utilizado para monitoramento de performance, resolução de incidentes, ajustes e proposição de melhorias em perfis de segurança (IPS, Antivírus, Filtro de URL) e inspeção SSL.

5.4.2. Na ocorrência de erros críticos, o prazo de 10 dias úteis será automaticamente interrompido e estendido.

5.4.3. O profissional técnico da CONTRATADA só será liberado da operação assistida presencial após o ambiente operar por, no mínimo, 05 (cinco) dias úteis consecutivos sem a ocorrência de qualquer erro crítico.

5.4.4. Caso ocorra uma falha crítica durante o período de estabilização, a contagem dos 5 dias uteis de "silêncio de erros" será reiniciada após a resolução definitiva do problema.

5.4.5. Relatório e Aceite: Ao final do período, deverá ser entregue um relatório de estabilização com os ajustes realizados. A aceitação definitiva da solução fica condicionada ao cumprimento integral deste ciclo de estabilização sem pendências.

5.5. O planejamento dos serviços de instalação deve resultar em um documento tipo SOW (em tradução livre, declaração de trabalho). Este documento deve conter:

5.5.1. Relação de produtos;
5.5.2. Descrição e quantidades de equipamentos e serviços;
5.5.3. Descrição da infraestrutura atual e desejada;
5.5.4. Detalhamento dos serviços que serão executados;
5.5.5. Premissas do projeto;
5.5.6. Local, horários e condições de execução dos serviços;
5.5.7. Pontos de contato da CONTRATANTE e CONTRATADA;
5.5.8. Cronograma faseado do projeto, divido em etapas, com responsáveis, data de início e fim (se aplicável);
5.5.9. Relação da documentação a ser entregue ao final da execução dos serviços;
5.5.10. Responsabilidades da CONTRATANTE e CONTRATADA;
5.5.11. Plano de gerenciamento de mudanças;
5.5.12. Plano de contingência/Rollback
5.5.13. Itens excluídos no projeto;

5.5.14. Termo de aceite.

5.6. Os serviços não poderão ser iniciados antes da apresentação e assinatura da declaração de trabalho (SOW), mediante concordância de ambas as partes.

5.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada.

5.8. Durante toda a implantação do projeto, o técnico da CONTRATADA deverá demonstrar aos técnicos da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (handover). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas e a operação dos principais recursos dos produtos ofertados.

6. REQUISITOS DE QUALIDADE E SEGURANÇA

6.1. A solução proposta deverá atender aos mais altos padrões de qualidade e segurança, garantindo a proteção dos ativos de informação do SESI-SP e SENAI-SP.

6.2. Conformidade: A solução deve estar em conformidade com as principais certificações de segurança e padrões da indústria (e.g., Common Criteria, FIPS, ISO 27001).

6.3. Resiliência: O hardware deve ser projetado para operação contínua 24x7, com componentes redundantes e capacidade de failover rápido em caso de falha.

6.4. Atualizações de Segurança: O fabricante deve prover atualizações de firmware e de inteligência de ameaças de forma contínua e automatizada.

6.5. Auditoria e Logs: A solução deve registrar eventos de segurança detalhados, permitindo auditorias completas e investigações de incidentes.

6.6. Proteção contra Ameaças Avançadas: Capacidade de detectar e mitigar ameaças persistentes avançadas (APTs), ataques de dia zero e ransomware.

6.7. Escalabilidade: A arquitetura da solução deve permitir a expansão futura de capacidade e funcionalidades sem a necessidade de substituição completa do hardware.

7. DO ACORDO DE NÍVEL DE SERVIÇO (ANS)

7.1. A **fabricante** deverá garantir um nível de serviço que assegure a máxima disponibilidade e desempenho da solução, conforme os seguintes parâmetros mínimos:

7.1.1. Cobertura do forticare: o SLA aqui descrito é complementado e garantido pelo serviço de suporte forticare compatível com o firewall, que deve ser parte integrante da contratação, assegurando a manutenção, atualizações e suporte técnico direto do fabricante.

7.1.2. Disponibilidade da solução (uptime): mínimo de 99,99% anual para o cluster de HA.

7.1.3. Tempo de resposta para incidentes críticos (severidade 1): contato inicial: máximo de 1 hora.

7.1.3.1. Início da resolução: máximo de 2 horas.
7.1.3.2. Resolução ou workaround: máximo de 4 horas.

7.1.4. Tempo de resposta para incidentes graves (severidade 2): contato inicial: máximo de 2 horas.

7.1.4.1. Início da resolução: máximo de 4 horas.
7.1.4.2. Resolução ou workaround: máximo de 8 horas.

7.1.5. Tempo de resposta para incidentes médios (severidade 3): contato inicial: máximo de 4 horas.

7.1.5.1. Início da resolução: máximo de 8 horas.
7.1.5.2. Resolução ou workaround: máximo de 24 horas.

7.2. Suporte técnico: disponibilidade de suporte técnico especializado 24x7x365, em português, para hardware e software, exclusivamente através do serviço forticare adquirido para a solução de firewall.

7.3. Substituição de hardware: em caso de falha de hardware, o fornecedor deverá garantir a substituição da peça ou equipamento em até 24 horas (next business day - nbd), em conformidade com o nível de serviço forticare.

7.4. Em caso de descumprimento do item 7.1.2, serão aplicadas as glosas conforme a seguir:

Nível de Serviço Descumprido	Percentual de Glosa sobre o Valor do contrato
Disponibilidade entre 99,90% e 99,98%	2%
Disponibilidade entre 99,00% e 99,89%	5%
Disponibilidade abaixo de 99,00%	10%

8. DO TREINAMENTO

8.1. Treinamento da solução fornecida a ser ministrado pela CONTRATADA, antes da etapa de migração do ambiente da CONTRATANTE.

8.2. O(s) instrutor(es) indicado(s) deverão apresentar certificação técnica oficial, devidamente comprovada e emitida pelo fabricante, atestando proficiência na solução objeto deste Memorial Descritivo.

8.3. Carga horária mínima de 20 (vinte) horas aula (podendo ser realizado em uma ou duas semanas a critério da CONTRATANTE.

8.4. Treinamento a ser realizado para até 5 (cinco) participantes;

8.5. Todo o ambiente de treinamento deverá ser preparado e fornecido pela CONTRATADA e deverão ser abordados conceitos teóricos e atividades práticas de laboratório.

8.6. Deverá ser abordado, no mínimo, os seguintes tópicos:

8.6.1. Configurações iniciais;
8.6.2. Configurações de VLANs, LACP, DHCP e tipos NAT;
8.6.3. Políticas de segurança;
8.6.4. Prevenção de ameaças, anti-malware, filtro URL e controle de aplicações;
8.6.5. Identificação de usuários, qualidade de serviço e regras por aplicação;
8.6.6. Filtro de dados e inspeção SSL;
8.6.7. VPN Site-to-Site e Client-To-Site;
8.6.8. Alta disponibilidade;
8.6.9. Gerenciamento e relatórios;
8.6.10. Backup e restore, atualizações (upgrade/patching);
8.6.11. Integrações com diretórios para autenticações;
8.6.12. Avaliação de boas práticas, verificação de logs;
8.6.13. Otimização de políticas de firewall e monitoramento de performance;
8.6.14. Suporte técnico (instruções de abertura de chamados com o fabricante e a CONTRATADA)
8.6.15. Abordagem teórica de todos os aspectos envolvidos no processo de migração de configurações e regras de firewall, incluindo a abordagem das configurações do recurso SASE.
8.6.16. Abordagem teórica e funcionalidades na ativação e sustentação de ambiente em alta disponibilidade Ativo-Ativo / Ativo-Passivo.

8.7. Todo o treinamento poderá ser realizado de forma remota, presencial ou híbrido a critério da CONTRATANTE.

8.8. As aulas remotas deverão ser gravadas e disponibilizadas, em até 5 dias uteis, para a equipe da CONTRATANTE.

8.9. O idioma das aulas deverá ser em português.

8.10. Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.

8.11. Deverá ser fornecido certificado de participação do treinamento aos participantes que frequentarem pelo menos 75% do total de horas.

8.12. Ao concluir o treinamento, os participantes deverão responder a um questionário de avaliação sobre o conteúdo ministrado e a qualidade geral (escala: péssimo a muito bom). Caso algum tópico previsto não tenha sido abordado, este deverá ser ministrado em até 2 dias úteis. Se

a avaliação geral for "Regular", "Ruim" ou "Péssimo", o curso será repetido com outro instrutor, em até 5 dias úteis e integralmente, até que se atinja o conceito "Bom" ou "Muito Bom", seguido de nova avaliação.

9. DOS PRAZOS

9.1. O prazo máximo para a implantação completa da solução, incluindo fornecimento, treinamento, instalação, configuração e migração de regras e testes de validação, será de 45 (quarenta e cinco) dias úteis, contados a partir da assinatura do contrato ou da emissão da Ordem de Serviço.

10. DA VIGÊNCIA CONTRATUAL

10.1. O prazo de vigência contratual será de 05 (cinco) anos, contados da assinatura, podendo ser prorrogado mediante justificativa e formalização de termo aditivo, observados os requisitos e limites previstos nos artigos 34, II, e 38 do Regulamento para Contratação e Alienação – RCA do SESI e do SENAI, inclusive quanto à necessidade de justificativa que ateste a manutenção da vantajosidade das condições e dos preços contratados após os 5 (cinco) anos iniciais, permitida a negociação com a CONTRATADA ou a extinção contratual sem ônus para qualquer das partes, nos termos do referido Regulamento.

10.2. Após o 12º mês de vigência contratual, **exclusivamente para o item 03, da lista de materiais prevista no subitem 4.2, do memorial descritivo**, poderá ser aplicado o reajustamento de preço, com base no índice IPCA/IBGE acumulado nos últimos 12 meses, relativo ao mês anterior (11º mês), ou, mediante concordância entre as partes, referente ao segundo mês anterior ao 12º (10º mês), ou ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

11. OBRIGAÇÕES DA CONTRATADA

11.1. Cumprir todas as obrigações, sem prejuízo de outras que venham a ser estabelecidas em contrato, como segue:

11.1.1. Ser parceira autorizada do fabricante Fortinet, em nível compatível com a implantação de soluções corporativas de segurança da informação, devidamente comprovado por documentação oficial do fabricante;
11.1.2. Possuir experiência comprovada na implantação de soluções de segurança baseadas em Next-Generation Firewall (NGFW), Secure SD-WAN, Secure Access Service Edge (SASE) e gerenciamento centralizado, compatíveis em porte e complexidade com o objeto desta contratação;
11.1.3. Dispor de estrutura técnica, operacional e de governança capaz de executar serviços de planejamento, implantação, configuração, integração, testes, documentação e estabilização da solução;
11.1.4. Possuir capacidade de interação e acionamento do suporte oficial do fabricante, quando necessário, utilizando canais e processos homologados;
11.1.5. Comprometer-se a executar a implantação em conformidade com as boas práticas, guias de arquitetura e recomendações oficiais do fabricante, visando segurança, desempenho, escalabilidade e manutenibilidade da solução;

11.1.6. Fornecer treinamento prévio adequado, conforme especificado nesse memorial descritivo, permitindo nivelamento técnico e entendimento da solução por toda equipe técnica do SESI-SP e SENAI-SP.
11.1.7. Fornecer os equipamentos novos, lacrados, com todos os seus acessórios e componentes para interligação de rede e elétrica, conforme as especificações técnicas detalhadas neste Memorial Descritivo.
11.1.8. Entregar os equipamentos no local indicado pelo SESI-SP e SENAI-SP, dentro do prazo estabelecido no cronograma de projeto.
11.1.9. Realizar a instalação física dos equipamentos na Sede do SESI-SP e SENAI-SP, incluindo a montagem em rack e conexão de cabos de rede e energia.
11.1.10. Executar a importação e migração das regras do firewall existente para o novo firewall, garantindo a transição segura e sem interrupções, havendo o handover, permitindo a consolidação do aprendizado técnico pela equipe do SESI-SP e SENAI-SP com explicações detalhadas de toda as ações de configuração no momento da execução das atividades.
11.1.11. Realizar toda a configuração necessária para entregar o firewall funcionando e operacional em cluster de Alta Disponibilidade (HA) Ativo-Ativo, conforme as melhores práticas do fabricante e as necessidades de segurança e rede do SESI-SP e SENAI-SP, incluindo a integração com o FortiManager e FortiAnalyzer existentes.
11.1.12. Executar testes, ajustes e validações da solução, comprovando o atendimento às especificações técnicas, aos requisitos de segurança e disponibilidade, e garantindo a entrega final da solução em pleno funcionamento.
11.1.13. Ativar e registrar todas as licenças de software e de serviço para toda a solução.
11.1.14. Disponibilizar documentação técnica completa da instalação e configuração realizada, incluindo diagramas de rede e manuais de operação.
11.1.15. Garantir a compatibilidade e integração da solução com a infraestrutura de rede e segurança existente do SESI-SP e SENAI-SP.
11.1.16. Disponibilizar equipe técnica para a execução dos serviços nos dias escolhidos pela CONTRATANTE, inclusive em finais de semana e fora do horário comercial, desde que a CONTRATANTE comunique a CONTRATADA com antecedência mínima de 24 horas;
11.1.17. Submeter-se, dentro do escopo e das cláusulas pactuadas no contrato, às determinações da Gerência Sênior de Tecnologia da Informação do SESI-SP e SENAI-SP, às suas normas e procedimentos, e prestar as informações e esclarecimentos que venham a ser solicitados;
11.1.18. Manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas no processo de seleção, necessárias para que todos os níveis de serviços acordados sejam cumpridos com utilização eficiente dos recursos disponíveis;
11.1.19. Manter os seus profissionais atualizados tecnologicamente, promovendo os treinamentos e participações em eventos de caráter técnico que permitam a prestação dos serviços, descritos neste memorial e seus anexos, em regime de excelência;
11.1.20. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando forem vítimas os seus técnicos no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;
11.1.21. Responsabilizar-se pelo cumprimento das exigências legais no que respeita às jornadas das equipes de trabalho, em seus diversos horários;

11.1.22. Assumir a responsabilidade por todos os encargos fiscais, previdenciários e obrigações previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria;
11.1.23. Responsabilizar-se pelos danos financeiros ou de imagem causados diretamente ao SESI-SP e SENAI-SP ou a terceiros, até o limite do contrato, decorrentes de sua culpa ou dolo quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou ao acompanhamento pela Gerência Sênior de Tecnologia da Informação do SESI-SP e SENAI-SP;
11.1.24. Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade do SESI-SP e SENAI-SP, além daqueles processados e gerados no ambiente físico da CONTRATADA, reconhecendo serem estes de propriedade exclusiva do SESI-SP e SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros;
11.1.25. Apresentar, quando solicitado, a licença de uso ou certificação de posse de todos os softwares de sua propriedade que serão empregados na prestação dos serviços, não cabendo ao SESI-SP e SENAI-SP quaisquer ônus decorrentes do uso indevido de softwares pela equipe técnica da CONTRATADA;
11.1.26. Responsabilizar-se pelo cumprimento da legislação competente por qualquer item de reparo no ambiente, não cabendo ao SESI-SP e SENAI-SP quaisquer ônus decorrentes;
11.1.27. Cumprir demais obrigações descritas no Chamamento Público e na minuta de contrato.

12. OBRIGAÇÕES DO SESI-SP E SENAI-SP

12.1. Deverá cumprir as seguintes obrigações, sem prejuízo de outras que venham a ser estabelecidas em contrato:

12.1.1. Disponibilizar o ambiente físico adequado (espaço em rack, energia elétrica, climatização e conectividade de rede) para a instalação dos equipamentos previstos nessa solução;
12.1.2. Indicar um ponto focal técnico para acompanhar a instalação, configuração e testes da solução;
12.1.3. Fornecer as informações e acessos necessários para a integração da solução com a infraestrutura existente, sob a supervisão de sua equipe técnica;
12.1.4. Comunicar a CONTRATADA com antecedência mínima de 24 horas caso a execução dos serviços seja solicitada em finais de semana ou fora do horário comercial;
12.1.5. Realizar a avaliação e o aceite formal da solução após o atingimento de:
12.1.5.1. Conclusão do treinamento;
12.1.5.2. Conclusão da migração;
12.1.5.3. Entrega da documentação de declaração de trabalho e as-built;
12.1.5.4. Relatório de ajustes e ausência de erros críticos, por 5 (cinco) dias seguidos, após a migração;
12.1.6. Efetuar os pagamentos devidos à CONTRATADA nos prazos e condições estabelecidos em contrato;
12.1.7. Colaborar com a CONTRATADA para a resolução de eventuais problemas ou impedimentos que possam surgir durante a execução do contrato;

12.1.8. Especificar e estabelecer normas e diretrizes para execução dos serviços ora contratados, definindo as prioridades e regras de atendimento, bem como os prazos e etapas para cumprimento das obrigações;
12.1.9. Fornecer à CONTRATADA, em tempo hábil, as informações necessárias à execução dos serviços, bem como a documentação técnica referente aos padrões adotados pelas CONTRATANTES;
12.1.10. Informar à CONTRATADA as normas e procedimentos de acesso às instalações das CONTRATANTES e eventuais alterações;
12.1.11. Permitir o acesso dos técnicos da CONTRATADA aos equipamentos e sistemas das CONTRATANTES necessários para execução dos serviços no ambiente computacional.

13. DA ABRANGÊNCIA DOS CUSTOS E RESPONSABILIDADES FINANCEIRAS

13.1. A CONTRATADA declara estar ciente de que todos os custos decorrentes da execução integral do objeto deste processo de seleção incluídos no valor global proposto.

13.2. Estão compreendidos no preço, sem ônus adicional ao CONTRATANTE, todos os custos diretos e indiretos relativos a:

13.2.1. Fornecimento de Solução: Hardware, softwares, licenças e acessórios previstos neste termo de referência;
13.2.2. Serviços Profissionais: Instalação, configuração, migração crítica de dados/regras e operação assistida;
13.2.3. Capacitação: Horas técnicas, materiais didáticos e certificações (se houver) para o treinamento operacional da equipe;
13.2.4. Encargos e Tributos: Todos os impostos (federais, estaduais e municipais), taxas, contribuições sociais e fiscais incidentes;
13.2.5. Logística e Pessoal: Despesas com deslocamento, hospedagem, alimentação, seguros, encargos trabalhistas e previdenciários de sua equipe técnica.

13.3. Eventuais omissões na proposta comercial ou subestimação de insumos necessários para a plena operacionalidade da solução serão de inteira responsabilidade da CONTRATADA, não cabendo qualquer pleito de ressarcimento ou aditivo financeiro por itens essenciais à entrega do objeto contratado.

14. GESTÃO E FISCALIZAÇÃO DO CONTRATO

14.1. O SESI-SP e SENAI-SP indicarão um colaborador em nível de gestão para atuar como representante do contrato, incumbido das seguintes atribuições:

14.1.1. Inteirar-se em detalhes de todas as cláusulas e condições do instrumento contratual e seus anexos, consultando, se necessário, os órgãos técnicos do SESI-SP e SENAI-SP quanto aos aspectos relacionados ao objeto do contrato, de forma a que sejam cumpridas, pela CONTRATADA, todas as cláusulas contratuais;
14.1.2. Coordenar a fiscalização da execução física e financeira do contrato;

14.1.3. Coordenar a fiscalização dos níveis de serviços acordados, quanto aos aspectos relacionados aos indicadores de qualidade e desempenho, bem como os quantitativos relativos aos serviços;
14.1.4. Colaborar com a CONTRATADA sugerindo melhorias nos métodos de trabalho e exercendo fiscalização preventiva, de preferência, à fiscalização corretiva;
14.1.5. Analisar e aprovar os relatórios gerenciais de serviços;
14.1.6. Solicitar posicionamento do seu superior nas decisões e providências que ultrapassarem sua competência, em tempo hábil, para adoção das medidas convenientes;
14.1.7. Solicitar alteração, inclusão ou exclusão ou alteração dos acordos de níveis de serviço (SLA) com base nas reuniões de análise.

ANEXO C

MODELO DE PROPOSTA COMERCIAL

(usar papel timbrado da EMPRESA)

CHAMAMENTO PÚBLICO N.º 494/2026

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO, INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE DO TIPO NEXT GENERATION *FIREWALL* (NGFW) E RECURSOS DE SEGURANÇA, PARA ATENDIMENTO DAS NECESSIDADES DO SESI-SP E DO SENAI-SP

PROPOSTA COMERCIAL ESCRITA	
Razão Social:	CNPJ:
Endereço completo:	
Telefone/Fax:	E-mail:

LOTE 01

ITEM	DESCRIÇÃO	PARTNUM.	ENTIDADE	QTDE.	PARCELA	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	FortiGate-201G	FG-201G	SESI	1	Única		
			SENAI	1	Única		
02	FortiGate-201G UTP License for **5 years**	FC-10-F2H1G-950-02-60	SESI	1	Única		
			SENAI	1	Única		
03	FW201G SASE 10 user access for **1 Year** per FW	FC-10-F2H1G-1329-02-12	SESI	1	Única		
			SENAI	1	Única		
04	NGFW 201G - RMA Next Day for **5 years**	FC-10-F2H1G-210-02-60	SESI	1	Única		
			SENAI	1	Única		
05	1GE SFP SX transceiver module	FN-TRAN-SX	SESI	4	Única		
			SENAI	4	Única		
06	10GE SFP+ transceiver module, short range	FN-TRAN-SFP+SR	SESI	6	Única		
			SENAI	6	Única		
07	FortiManager - VM License	FMG-VM-10-UG	SESI	1*	Única		
			SENAI		Única		
08	FortiManager - VM FortiCare Premium Support for 5 years	FC1-10-M3004-248-02-60	SESI	1*	Única		
			SENAI		Única		
09	Treinamento Técnico	Serviço	SESI	1*	Única		
			SENAI		Única		
10	Serviço de Implementação da solução / Migração	Serviço	SESI	1*	Única		
			SENAI		Única		
VALOR TOTAL PARA 60 MESES DE CONTRATO							

* Prezado(a) fornecedor(a), considerando que os serviços serão compartilhados entre as Entidades, os valores unitários correspondentes aos itens 07 a 10 deverão ser rateados igualmente entre SESI-SP e SENAI-SP, na proporção de 50% para cada Entidade.

1. A proposta deverá contemplar, obrigatoriamente, o valor total da contratação para o período de **60 (sessenta) meses**, considerando todos os fornecimentos, serviços, licenças, equipamentos, instalação, configuração, migração, treinamento, suporte e demais obrigações previstas neste processo de seleção.

1.1. O item 03 da proposta deverá considerar o valor total para 12 (doze) meses de contrato, em atendimento ao item 11.6.1. do Chamamento Público.

2. Os pagamentos serão realizados conforme as etapas de execução e condições estabelecidas no item 15.1.3. do Chamamento Público, mediante o cumprimento das obrigações correspondentes e o aceite dos serviços e/ou fornecimentos pelo SESI-SP e SENAI-SP.

3. Nos valores apresentados estão incluídas todas as despesas necessárias à execução integral do objeto, incluindo, custos com transporte, logística, entrega, instalação, configuração, migração, treinamento, licenciamento, suporte, tributos, encargos trabalhistas, previdenciários, fiscais e comerciais, seguros e quaisquer outras despesas incidentes ou necessárias ao cumprimento das obrigações contratuais.

4. A CONTRATADA deverá executar o objeto em estrita conformidade com as especificações técnicas, prazos, condições e demais requisitos estabelecidos neste processo de seleção, não sendo admitida a cobrança de custos adicionais ao SESI-SP e SENAI-SP decorrentes de obrigações já previstas no escopo da contratação, durante o período de vigência contratual.

5. A CONTRATADA deverá emitir Notas Fiscais distintas para o SESI-SP e para o SENAI-SP, de acordo com a natureza dos fornecimentos e serviços efetivamente executados, observando os respectivos pedidos de compra.

6. A empresa deverá informar a modalidade de garantia de execução contratual, conforme condições estabelecidas no Chamamento Público:

( ) Caução em dinheiro
( ) Fiança Bancária
( ) Seguro-Garantia

(Local e Data)

_____

(Nome completo, CPF e assinatura do representante legal)

CARIMBO DE CNPJ DA EMPRESA

ANEXO D

MINUTA DE CONTRATO

CONTRATO DE PRESTAÇÃO DE SERVIÇOS DE FORNECIMENTO, INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE DO TIPO NEXT GENERATION FIREWALL (NGFW) E RECURSOS DE SEGURANÇA PARA O SESI-SP E O SENAI-SP

Pelo presente instrumento particular e na melhor forma de direito, em que são partes, de um lado, o SERVIÇO SOCIAL DA INDÚSTRIA – SESI, Departamento Regional de São Paulo, inscrito no CNPJ sob o nº 03.779.133/0001-04, e o SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI, Departamento Regional de São Paulo, inscrito no CNPJ sob o nº 03.774.819/0001-02, ambos com sede nesta Capital do Estado de São Paulo, na Avenida Paulista, nº 1313, 3º andar, Bairro Bela Vista, CEP 01311-923, neste ato representados por seu Gerente Sênior de Tecnologia da Informação, Glauber Magalhães de Souza, a seguir denominados, simplesmente, SESI-SP e SENAI-SP; e, de outro lado, , inscrita no CNPJ sob o nº , com sede na , nº , bairro , CEP , na cidade de , Estado de , aqui representada em conformidade com seus atos constitutivos, a seguir denominada simplesmente CONTRATADA, resolvem celebrar o presente contrato, mediante as seguintes cláusulas e condições que, mutuamente, aceitam e outorgam.

Cláusula Primeira – Do Objeto

1.1. Por meio do presente instrumento, a CONTRATADA se obriga à prestação de serviços de fornecimento, treinamento, instalação, configuração e migração de solução de segurança de rede do tipo *Next Generation Firewall (*NGFW*)* e recursos de segurança, da fabricante *FORTINET*, para atendimento das necessidades do SESI-SP e do SENAI-SP, Lote(s)_____, nos termos do Chamamento Público do Processo de Seleção Com Disputa Aberta - PSDA nº 494/2026, Memorial Descritivo e demais anexos.

1.2. Fazem parte, ainda, do presente Contrato, independentemente de transcrição, os seguintes documentos:

a) Regulamento Para Contratação e Alienação – RCA do SESI e do SENAI;
b) Chamamento Público – PSDA nº 494/2026, Memorial Descritivo, com seus respectivos anexos;
c) Proposta apresentada pela CONTRATADA com data __/___/____, no que não contrarie o presente contrato e os demais documentos.

1.3. As especificações dos serviços encontram-se previstas em sua integralidade no Memorial Descritivo, do PSDA citado, parte integrante deste ajuste.

Cláusula Segunda – Da Vigência/Prazos e Reajuste

2.1 O prazo de vigência deste contrato será de 05 (cinco) anos, contados da assinatura, podendo ser prorrogado mediante justificativa e formalização de termo aditivo, observados os requisitos e limites previstos nos artigos 34, II, e 38 do Regulamento para Contratação e Alienação – RCA do SESI e do SENAI, inclusive quanto à necessidade de justificativa que ateste a manutenção da vantajosidade das condições e dos preços contratados após os 5 (cinco) anos iniciais, permitida a negociação com a CONTRATADA ou a extinção contratual sem ônus para qualquer das partes, nos termos do referido Regulamento.

2.2 A pedido da CONTRATADA, após o 12º mês de vigência contratual, **exclusivamente para o item 03, da lista de materiais prevista no subitem 4.2, do memorial descritivo**, poderá ser aplicado o reajustamento de preço, com base no índice IPCA/IBGE acumulado nos últimos 12 meses, relativo ao mês anterior (11º mês), ou, mediante concordância entre as partes, referente ao segundo mês anterior ao 12º (10º mês), ou ainda, por outro índice que venha a substituí-los, caso haja a extinção de um deles.

Cláusula Terceira – Do Preço, Forma de Pagamento e Reajuste

3.1. O valor total estimado a ser pago pela prestação dos serviços pelos 05 (cinco) anos pactuado é de até R$, conforme proposta apresentada pela CONTRATADA, ora elencada no Anexo I deste ajuste.

3.1.1. Nos preços referidos na cláusula 3.1, supra, estão inclusos todos os custos inerentes à prestação dos serviços contratados, sem exceção, inclusive de todos os tributos, impostos, taxas, salários, encargos sociais, previdenciários, trabalhistas e rescisórios dos empregados da CONTRATADA, bem como seguros, alimentação, uniforme/fardamento, transporte de qualquer natureza, combustível, equipamentos, materiais, inclusive ferramentas e utensílios, depreciação, aluguéis, administração, lucro e quaisquer outras despesas, sejam diretas ou indiretas, conforme previsto no Memorial Descritivo, do Chamamento Público - PSDA nº 494/2026.

3.2. Serão realizados os pagamentos apenas dos serviços efetivamente realizados.

3.3. Os pagamentos serão efetuados em até 15 (quinze) dias corridos, contados da apresentação da respectiva nota fiscal/fatura, acompanhada dos relatórios técnicos e demais documentos necessários à validação dos serviços executados no período, fora a dezena, de modo que ocorram nos dias 10, 20 ou 30.

3.4. Quando essas datas recaírem em finais de semana ou feriados, o pagamento será efetuado no primeiro dia útil subsequente. No mês de fevereiro, os pagamentos serão realizados nos dias 10, 20 e 28, ou 29, em caso de ano bissexto.

3.5. O(s) pagamento(s) deverão ser rateados entre o SESI-SP e o SENAI-SP, observando-se a participação de cada entidade na contratação, na execução do objeto e na destinação dos itens e serviços, conforme definido no PSDA nº 494/2026, na proposta comercial e neste ajuste.

3.6. Após a aceitação dos serviços pelo SESI-SP e pelo SENAI-SP, a CONTRATADA deverá emitir faturas individuais para cada pedido de compra, conforme a etapa concluída:

Etapa	Descrição da Execução	Prazo Estimado para a Execução	Valor a ser pago
1	Entrega e instalação dos equipamentos: • **FortiGate-201G** (item 01 do Anexo I) • **1GE SFP SX transceiver module** (item 05 do Anexo I) • **10GE SFP+ transceiver module, short range** (item 06 do Anexo I)	Até **15 (quinze) dias úteis** após o recebimento do respectivo Pedido de Compra.	Parcela única, correspondente a 50% do valor total contratado
2	Ativação das licenças/suporte, implantação, migração, conclusão do período de operação assistida e aceitação final da solução.	Até 30 (trinta) dias úteis após o recebimento do respectivo Pedido de Compra.	Parcela única, correspondente a 50% do valor contratado
3	Fornecimento: FortiManager - VM License	Conforme necessidade e ativação da licença, mediante Pedido de Compra.	Parcela Única
4	Fornecimento: FortiManager - VM FortiCare Premium Support for 5 years	Vigência de **60 (sessenta) meses**, conforme condições estabelecidas para o suporte contratado	Parcela Única
5	Treinamento Técnico	Conforme cronograma a ser definido entre as partes, após o recebimento do respectivo Pedido de Compra.	Parcela Única
6	Serviço de Implementação da solução / Migração	Conforme cronograma a ser definido entre as partes, após o recebimento do respectivo Pedido de Compra.	Parcela Única

3.7 Caso sejam identificadas pendências, inconformidades ou descumprimento de qualquer obrigação contratual, o pagamento poderá ser suspenso total ou parcialmente até a regularização, sem prejuízo da aplicação das penalidades cabíveis, inclusive glosas, quando previstas.

3.8 Para contagem do prazo de pagamento, considerar-se-á o dia da entrega da Nota Fiscal / Fatura, devidamente validada pelo Gestor do Contrato.

3.9 Os pagamentos serão efetuados através de depósito bancário, devendo ser encaminhadas, obrigatoriamente, as duplicatas e/ou recibos devidamente quitados. Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

3.10 A CONTRATADA deverá aplicar os descontos decorrentes das inconformidades detectadas pelo SESI-SP e pelo SENAI-SP, quando houver, em atendimento ao item 13.3. do Memorial Descritivo (Anexo B).

3.11 A CONTRATADA deverá manter, durante toda a vigência contratual, as condições de habilitação e regularidade exigidas para o recebimento dos valores contratados.

3.12 Os pagamentos serão efetuados, em moeda corrente nacional, estando os referidos pagamentos condicionados, além das exigências previstas, a aprovação dos serviços pelo SESI-SP e pelo SENAI-SP.

3.13 Não deverão ser emitidos boletos bancários, bem como, não é permitido negociar os títulos.

3.14 Na hipótese de ser apresentada a documentação de cobrança com erro ou incompleta ou se concretizando circunstância que impeça a liquidação das despesas, o pagamento será suspenso e o prazo de vencimento prorrogado, se necessário até que sejam providenciadas as medidas saneadoras cabíveis, inclusive emissão de novas faturas se for o caso não acarretando, neste caso, quaisquer ônus para o SESI-SP e para o SENAI-SP.

3.15 Caso a documentação para pagamento não seja entregue conforme previsto acima, o SESI-SP e o SENAI-SP poderão postergar o pagamento ficando estabelecido o vencimento da nota fiscal/fatura somente nos dias 10, 20 ou 30 do mês.

3.16 No caso de faturas que cheguem ao SESI-SP e ao SENAI-SP vencidas ou com prazo de pagamento inferior a 10 (dez) dias úteis, ou ainda as em que, nos casos de serem contestadas pelo SESI-SP e SENAI-SP, seja comprovada a correção dos valores, será facultado à CONTRATADA emitir novo documento de cobrança com nova data para pagamento, respeitando o prazo mínimo de 10 (dez) dias úteis entre a data do recebimento pelo SESI-SP e SENAI-SP e a nova data de pagamento ou, alternativamente, emitir documento que prorrogue a data de pagamento da fatura enviada.

3.17 Fica vedada a negociação de duplicatas com terceiros, bem como o desconto ou a promoção de cobrança através da rede bancária, bem como qualquer forma de cessão à terceiros.

3.18 O descumprimento do disposto acima acarretará a aplicação de penalidade(s) consignadas neste instrumento

3.19 Se da infringência no disposto na subcláusula 3.18, advier protesto da duplicata, a CONTRATADA, além da penalidade citada acima, se obriga a efetuar às suas expensas, o respectivo cancelamento, no prazo máximo de 05 (cinco) dias, contados da data da emissão do correspondente instrumento cartorário.

3.20 Por força das legislações vigentes, se for o caso, o SESI-SP e SENAI-SP reterão do valor bruto da nota fiscal, as alíquotas pertinentes aos tributos a seguir discriminados:

a. Imposto de Renda;
b. INSS;
c. ISS (imposto sobre serviços de qualquer natureza);
d. CSLL (contribuição social sobre lucro líquido);
e. COFINS; e
f. PIS.

3.21 Quando da emissão da nota fiscal, a CONTRATADA deverá destacar o valor das retenções dos tributos referidos na subcláusula acima.

3.21.1 No caso da CONTRATADA ser beneficiada com decisão judicial que dispense a obrigatoriedade de retenção e recolhimento na fonte de qualquer dos tributos acima relacionados, deverá providenciar Ofício Judicial ao SESI-SP e ao SENAI-SP para que cumpra a decisão judicial ou, na impossibilidade de oficiar o SESI-SP e SENAI-SP,

deverá apresentar cópias autenticadas da petição inicial, da liminar, da sentença, do acórdão e outros documentos que o SESI-SP e SENAI-SP julgarem necessários, bem como, providenciar, trimestralmente, Certidão de Objeto e Pé que comprove estar a decisão ainda em vigor na data do pagamento.

3.22 O SESI-SP e SENAI-SP se reservam, ainda, o direito de reter quaisquer importâncias referentes a outros impostos, taxas, contribuições e recolhimentos obrigatórios, incidentes sobre a prestação dos serviços ora contratados.

3.23 A CONTRATADA não terá direito ao recebimento de valores antecipados em decorrência da prestação dos serviços.

3.24 O SESI-SP e SENAI-SP poderão suspender o pagamento de qualquer nota fiscal apresentada pela CONTRATADA, no todo ou em parte, nos seguintes casos:

3.24.1 Descumprimento de obrigação relacionada com os serviços contratados;
3.24.2 Não cumprimento de obrigação contratual, hipótese em que o pagamento ficará retido até que a CONTRATADA atenda à cláusula infringida;
3.24.3 Obrigações da CONTRATADA com terceiros que, eventualmente, possam prejudicar o SESI-SP e o SENAI-SP;
3.24.4 Paralisação dos serviços por culpa da CONTRATADA; e
3.24.5 Nos casos de suspensão dos serviços decorrente de determinação de órgão governamental que impeça a sua realização, ou que os procedimentos a serem adotados para sua realização não possam ser cumpridos pelo SESI-SP/SENAI-SP, assegurado o pagamento dos serviços executados.

3.25 A CONTRATADA não poderá pleitear perante o SESI-SP e o SENAI-SP o repasse ao preço aqui estipulado, de qualquer tributo ou outro encargo, que venham a ser majorados no curso da prestação dos serviços.

3.26 O SESI-SP e o SENAI-SP poderão deduzir da fatura os valores correspondentes aos descontos de pagamento e penalidades.

Cláusula Quarta – Das Obrigações da CONTRATADA

4.1 São obrigações da CONTRATADA:

4.1.1. Executar o objeto deste contrato em conformidade com as condições, os prazos, as especificações técnicas e os requisitos estabelecidos neste instrumento, bem como no PSDA nº 494/2026, memorial descritivo e demais anexos.
4.1.2. Fornecer os equipamentos novos, lacrados e acompanhados de todos os acessórios e componentes necessários à interligação de rede e elétrica, conforme as especificações técnicas contratadas.
4.1.3. Entregar os equipamentos nos locais indicados pelo SESI-SP e pelo SENAI-SP, observados os prazos estabelecidos no cronograma de execução.
4.1.4. Realizar a instalação física dos equipamentos nos locais indicados pelo SESI-SP e pelo SENAI-SP, incluindo a montagem em rack e a conexão dos cabos de rede e de energia.
4.1.5. Executar o planejamento, a configuração, a integração, os testes e a validação da solução, observando as boas práticas, os guias de arquitetura e as recomendações oficiais do fabricante, de modo a assegurar o atendimento aos requisitos técnicos, de segurança, desempenho e disponibilidade contratados.
4.1.6. Configurar e entregar a solução em funcionamento, em cluster de Alta Disponibilidade (HA) Ativo-Ativo, incluindo a integração com o FortiManager e o FortiAnalyzer existentes no ambiente do SESI-SP e do SENAI-SP.

4.1.7. Executar a importação e a migração das regras do firewall existente para a nova solução, adotando as medidas necessárias para assegurar a integridade das configurações e minimizar os riscos de indisponibilidade durante a transição.
4.1.8. Realizar os testes, ajustes e validações necessários à comprovação do funcionamento da solução e de sua conformidade com as especificações técnicas contratadas, corrigindo eventuais falhas identificadas.
4.1.9. Ativar e registrar as licenças de software e de serviços previstas na contratação, observados os respectivos períodos de vigência e as condições contratadas.
4.1.10. Fornecer treinamento técnico à equipe indicada pelo SESI-SP e pelo SENAI-SP, conforme as condições e o escopo estabelecidos nos anexos contratuais, incluindo as orientações necessárias à operação e à administração da solução.
4.1.11. Durante a implantação e a migração, compartilhar com a equipe técnica do SESI-SP e do SENAI-SP as informações necessárias à compreensão das configurações e dos procedimentos executados, de modo a possibilitar a transferência de conhecimento sobre a solução implementada.
4.1.12. Disponibilizar documentação técnica da solução implantada, incluindo as configurações realizadas, os diagramas de rede e os manuais de operação pertinentes.
4.1.13. Disponibilizar equipe técnica com capacidade para executar os serviços contratados nos dias e horários definidos de comum acordo com o SESI-SP e o SENAI-SP, inclusive em finais de semana e fora do horário comercial, quando necessário e mediante comunicação prévia de, no mínimo, 24 (vinte e quatro) horas, ressalvadas as situações emergenciais previstas contratualmente.
4.1.14. Disponibilizar suporte técnico, atualizações de segurança e demais serviços de suporte e manutenção previstos na contratação, durante os respectivos períodos de cobertura, observados os níveis de serviço e os prazos estabelecidos neste contrato e em seus anexos.
4.1.15. Providenciar a substituição dos equipamentos ou componentes abrangidos pela contratação, quando necessária, observadas as condições, a cobertura e os prazos de atendimento contratados.
4.1.16. Responsabilizar-se, com exclusividade, pela execução do objeto por seus empregados, prepostos, parceiros e terceiros por ela contratados, sem prejuízo das responsabilidades legal e contratualmente aplicáveis.
4.1.17. Arcar com os custos de transporte, deslocamento, estadia, alimentação e demais despesas necessárias à execução do objeto, quando aplicáveis e conforme as condições contratadas.
4.1.18. Comunicar por escrito ao gestor do contrato qualquer fato que possa comprometer ou impedir o cumprimento das obrigações, condições ou prazos contratuais, informando as providências adotadas para sua solução.
4.1.19. Corrigir, reparar ou solucionar, sem ônus adicional para o SESI-SP e o SENAI-SP, as falhas, os defeitos ou as desconformidades imputáveis à CONTRATADA identificados na execução do objeto, sem prejuízo das demais medidas previstas neste contrato.
4.1.20. Responsabilizar-se pelos danos e prejuízos causados ao SESI-SP, ao SENAI-SP ou a terceiros, quando decorrentes de ação ou omissão imputável à CONTRATADA, inclusive por atos de seus empregados, prepostos, parceiros e terceiros por ela contratados, sem que a fiscalização ou o acompanhamento da execução contratual excluam ou reduzam essa responsabilidade.
4.1.21. Manter, durante a vigência contratual, as condições de habilitação e qualificação exigidas para a contratação, bem como a regularidade fiscal, trabalhista e previdenciária, apresentando os documentos comprobatórios sempre que solicitados pelo SESI-SP e/ou pelo SENAI-SP.
4.1.22. Cumprir a legislação aplicável à execução do objeto, inclusive as disposições relativas à saúde e à segurança do trabalho, aos acidentes de trabalho, às jornadas de trabalho e às obrigações trabalhistas, previdenciárias, fiscais e comerciais relacionadas aos profissionais envolvidos na execução contratual.

4.1.23. Assumir, com exclusividade, os encargos e as obrigações decorrentes das relações mantidas com seus empregados, prepostos, parceiros e terceiros, inclusive aqueles decorrentes de acordos, dissídios e convenções coletivas de trabalho, sem transferência de responsabilidade ao SESI-SP e ao SENAI-SP, ressalvadas as hipóteses previstas em lei.

4.1.24. Observar as normas internas de segurança, acesso e funcionamento do SESI-SP e do SENAI-SP aplicáveis aos locais em que os serviços forem executados, bem como as orientações do gestor do contrato, desde que compatíveis com o objeto e com as disposições contratuais.

4.1.25. Prestar as informações e os esclarecimentos solicitados pelo gestor do contrato, bem como atender às orientações relacionadas à execução do objeto, observados o escopo e as condições contratadas.

4.1.26. Guardar sigilo sobre os dados, as informações, os documentos, as credenciais de acesso e os demais elementos a que tiver acesso em razão da execução contratual, utilizando-os exclusivamente para as finalidades relacionadas ao objeto e abstendo-se de divulgá-los, reproduzi-los, compartilhá-los ou disponibilizá-los a terceiros sem autorização, ressalvadas as hipóteses legalmente admitidas.

4.1.27. Reconhecer que os dados e as informações de titularidade do SESI-SP e do SENAI-SP, bem como os produtos e documentos por eles disponibilizados ou gerados em decorrência da execução contratual, permanecem sujeitos aos respectivos direitos de titularidade, observadas as disposições contratuais aplicáveis.

4.1.28. Utilizar softwares e demais recursos de terceiros em conformidade com as respectivas licenças e autorizações de uso, responsabilizando-se pelas irregularidades que lhe sejam imputáveis e pelos ônus delas decorrentes.

4.1.29. Manter profissionais tecnicamente capacitados e em número compatível com a execução do objeto, assegurando que possuam os conhecimentos necessários ao desempenho das atividades contratadas.

4.1.30. Arcar com os custos e adotar as providências de sua responsabilidade para a reparação de danos ao ambiente, aos equipamentos ou à infraestrutura do SESI-SP e do SENAI-SP decorrentes de sua atuação na execução contratual.

4.1.31. Submeter-se à fiscalização do SESI-SP e do SENAI-SP, prestando as informações necessárias ao acompanhamento da execução contratual e permitindo a verificação do cumprimento das obrigações assumidas, sem prejuízo de sua responsabilidade integral pela execução do objeto.

4.1.32. Apresentar, quando solicitado, os documentos comprobatórios das licenças de uso ou autorizações relativas aos softwares de sua propriedade ou de terceiros utilizados na execução do objeto.

4.1.33. Cumprir as demais obrigações previstas neste contrato e em seus anexos, no que forem aplicáveis ao objeto contratado.

4.1.34. Fornecer aos seus empregados e prepostos os uniformes, crachás de identificação e equipamentos de proteção individual (EPIs) necessários à execução dos serviços, quando aplicáveis, responsabilizando-se por sua utilização adequada e pelo cumprimento das normas de saúde e segurança do trabalho.

4.1.35. Assegurar que seus empregados e prepostos estejam devidamente identificados durante a permanência nas dependências do SESI-SP e do SENAI-SP, bem como cumpram as normas internas de segurança, acesso e circulação aplicáveis aos locais de execução dos serviços.

4.1.36. Cumprir a legislação relativa à proibição do trabalho infantil, não empregando menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, nem menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos, nos termos da legislação vigente.

4.1.37. Garantir que seus empregados e prepostos utilizem os equipamentos, ferramentas e materiais adequados à execução dos serviços, observando as normas técnicas e de segurança aplicáveis.

4.1.38. Ministrar o treinamento da solução fornecida antes da etapa de migração do ambiente do SESI-SP e SENAI-SP, observando a carga horária mínima de 20 (vinte) horas-aula, o limite de 5 (cinco) participantes e os demais requisitos, conteúdos, condições de realização e critérios de avaliação estabelecidos no Memorial Descritivo do PSDA nº 494/2026 e em seus anexos, incluindo a disponibilização de instrutor com certificação técnica oficial do fabricante, material didático e certificados de participação, bem como o cumprimento das medidas de complementação ou repetição do treinamento, quando aplicáveis.

4.1.39. Concluir a implantação da solução, incluindo fornecimento, treinamento, instalação, configuração, migração das regras e testes de validação, no prazo máximo de 45 (quarenta e cinco) dias úteis, contado da assinatura do contrato ou da emissão da Ordem de Serviço, conforme definido pelo SESI-SP e SENAI-SP.

4.1.40. Executar os serviços de forma coordenada, minimizando os impactos no ambiente de produção e preservando a continuidade dos serviços essenciais do SESI-SP e SENAI-SP.

4.1.41. Realizar operação assistida presencial por, no mínimo, 10 (dez) dias úteis após a migração e entrada em produção, observadas as condições de estabilização e aceite previstas no Memorial Descritivo.

4.1.42. Entregar, ao término da implantação, a documentação técnica final da solução, incluindo o relatório *as-built*, as configurações realizadas e as orientações necessárias à continuidade da operação.

4.1.43. Manter suporte técnico especializado, atualizações de segurança e garantia durante os períodos contratados, observados os níveis de serviço e os prazos de atendimento estabelecidos neste contrato e em seus anexos.

4.1.44. Observar as normas de confidencialidade, segurança da informação e proteção de dados pessoais aplicáveis à execução contratual.

4.1.45. Incluir no preço contratado todos os custos necessários à execução integral do objeto, não cabendo cobrança adicional por insumos ou atividades essenciais ao cumprimento das obrigações assumidas.

4.1.46. Apresentar, antes do início dos serviços, o plano de trabalho (SOW), com o cronograma, as etapas, as responsabilidades das partes e os procedimentos de contingência, para aprovação do SESI-SP e do SENAI-SP.

Cláusula Quinta – Demais Obrigações da CONTRATADA: Trabalhistas e Previdenciárias e Afins

5.1. A CONTRATADA deverá cumprir todas as obrigações trabalhistas e previdenciárias relativas aos profissionais designados para a prestação de serviço, observando, especialmente, as seguintes obrigações:

a) pagar os salários e demais verbas diretamente ao seu funcionário alocado a prestação de serviço;
b) observar as obrigações previstas na convenção, acordo coletivo, acórdão normativo ou na legislação incidente aplicável à categoria profissional do empregado, inclusive no que diz respeito a pisos salariais;
c) cumprir as obrigações trabalhistas de acordo com os valores e especificações indicados na planilha de custos e formação de preços contida na Proposta, sempre respeitados os mínimos previstos na norma coletiva aplicável;
d) atender a legislação relativa à segurança e à medicina do trabalho, e em particular as Normas Regulamentadoras (NR) expedidas pelo Ministério do Trabalho e Emprego;
e) pagar antecipadamente, em parcela única mensal, os insumos referentes a vale-transporte e auxílio-alimentação (se for o caso, ora quando aplicável).

5.2. Deve ser mantido e atualizado pela CONTRATADA, bem como exibidos por meio de cópias, sempre que solicitadas pelo SESI-SP e pelo SENAI-SP, os registros, anotações e documentos que comprovem o cumprimento das obrigações trabalhistas e previdenciárias e afins, tais como:

a) o contrato de trabalho, o regulamento interno da empresa, se houver, o acordo ou a convenção coletiva de trabalho, ou ainda, o acórdão normativo, se for o caso, relativos à categoria profissional do empregado;
b) o registro do empregado e Carteira de Trabalho e Previdência Social;
c) o Atestado de Saúde Ocupacional (ASO), comprovando a realização das avaliações médicas (admissional, periódica, demissional e, se for o caso, de retorno ao trabalho e de mudança de função) e exames complementares determinados pelo médico do trabalho;
d) documentos comprobatórios do pagamento das contribuições previdenciárias dos empregados e do empregador;
e) cartão, ficha ou livro de ponto assinado pelo empregado, ou documento comprobatório do registro eletrônico de ponto, nos quais constem as horas trabalhadas normais e extraordinárias, se for o caso;
f) recibo de concessão de aviso de férias, a ser dado 30 (trinta) dias antes do respectivo gozo;
g) documento comprobatório de depósito bancário na conta do trabalhador referente ao pagamento dos salários mensais e adicionais aplicáveis, férias acrescidas do terço constitucional e décimo terceiro salário (primeira e segunda parcelas);
h) documento comprobatório de fornecimento de auxílio-alimentação;
i) documento comprobatório do recolhimento dos valores devidos ao FGTS nas respectivas contas vinculadas do empregado;
j) termos que cuidem da demissão ou rescisão do contrato, sua respectiva homologação e quitação de verbas rescisórias, na forma da legislação;
k) documento comprobatório da concessão de aviso prévio pelo empregador ou pelo empregado e,
l) documento comprobatório da entrega dos documentos necessários à obtenção de seguro-desemprego pelo empregado, nas hipóteses em que o mesmo faça jus ao benefício.

5.3. Fica estabelecido que a CONTRATADA é a única e exclusiva empregadora dos profissionais por ela alocados para a execução dos serviços objeto deste contrato, inexistindo qualquer vínculo empregatício entre esses profissionais e o SESI-SP e SENAI-SP.

5.4. Compete ainda exclusivamente à CONTRATADA o cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais e comerciais decorrentes da relação de trabalho, inclusive aquelas oriundas de convenções, acordos ou dissídios coletivos. Caso o SESI-SP e o SENAI-SP venham a ser acionados judicialmente ou extrajudicialmente em razão de qualquer obrigação decorrente dessas relações, a CONTRATADA deverá assumir integralmente a responsabilidade pelo caso e ressarcir todas as despesas incorridas, incluindo custas, emolumentos, indenizações e honorários advocatícios.

5.5. O SESI-SP e o SENAI-SP poderão, a qualquer tempo, exigir a comprovação do cumprimento dessas obrigações, mediante apresentação dos documentos pertinentes, como condição para a liberação de pagamentos contratualmente devidos.

5.6. A CONTRATADA deverá apresentar certidões de antecedentes criminais atualizadas a cada 6 (seis) meses, relativas aos empregados, prepostos ou representantes que, em razão da execução dos serviços, tenham contato direto com crianças e adolescentes nas dependências

do SESI-SP e do SENAI-SP, inclusive aqueles vinculados a eventual subcontratada, observada a legislação aplicável.

5.6.1 A previsão justifica-se pela necessidade de reforçar a proteção integral de crianças e adolescentes, em observância ao art. 227 da Constituição Federal, aos arts. 4º e 5º do Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e ao art. 14 da Lei nº 14.811/2024, que prevê a manutenção de fichas cadastrais e certidões de antecedentes criminais atualizadas dos colaboradores que atuam em instituições que desenvolvem atividades com crianças e adolescentes. A exigência deverá observar a legislação aplicável e restringir-se aos profissionais que, em razão da execução contratual, tenham contato direto com esse público.

Cláusula Sexta – Das Obrigações do SESI-SP e do SENAI-SP

6.1 São obrigações do SESI-SP e do SENAI-SP:

6.1.1. Disponibilizar ambiente físico adequado à instalação dos equipamentos, incluindo espaço em rack, energia elétrica, climatização e conectividade de rede.

6.1.2. Indicar responsável técnico para acompanhar a instalação, a configuração, a migração e os testes da solução.

6.1.3. Fornecer as informações, os acessos e a documentação técnica necessários à integração da solução com a infraestrutura existente, observadas as normas e os procedimentos de segurança aplicáveis.

6.1.4. Comunicar à CONTRATADA, com antecedência mínima de 24 (vinte e quatro) horas, a necessidade de execução dos serviços em finais de semana ou fora do horário comercial.

6.1.5. Avaliar e realizar o aceite formal da solução após a conclusão do treinamento e da migração, a entrega da documentação técnica de declaração de trabalho e as-built, bem como a apresentação do relatório de ajustes e a verificação da ausência de erros críticos durante 5 (cinco) dias consecutivos após a migração.

6.1.6. Efetuar os pagamentos devidos à CONTRATADA, observados os prazos e as condições estabelecidos neste contrato.

6.1.7. Colaborar com a CONTRATADA na resolução de problemas ou impedimentos que possam surgir durante a execução contratual, no âmbito de suas atribuições.

6.1.8. Estabelecer as diretrizes e prioridades necessárias à execução dos serviços, definindo, em conjunto com a CONTRATADA, quando aplicável, os prazos e as etapas de execução, respeitadas as condições contratadas.

6.1.9. Fornecer à CONTRATADA, em tempo hábil, as informações e a documentação técnica referentes aos padrões adotados pelo SESI-SP e SENAI-SP, necessárias à execução do objeto.

6.1.10. Informar à CONTRATADA as normas e os procedimentos de acesso às instalações do SESI-SP e do SENAI-SP, bem como eventuais alterações.

6.1.11. Viabilizar o acesso dos profissionais da CONTRATADA aos equipamentos e sistemas necessários à execução dos serviços, mediante autorização prévia e observância das normas de segurança da informação, dos procedimentos internos e das regras de acesso do SESI-SP e do SENAI-SP.

Cláusula Sétima – Da Confidencialidade

7.1 A CONTRATADA deverá assinar o termo de confidencialidade do SESI-SP e do SENAI-SP, de forma a respeitar a confidencialidade, integridade e disponibilidade das informações relacionadas à prestação de serviços em questão, sob pena de multa e rescisão contratual.

7.2 As partes deverão manter completo e absoluto sigilo sobre quaisquer dados, materiais, informações, documentos, especificações técnicas e inovações que tenham acesso umas das outras, em virtude da prestação dos serviços objeto deste contrato, não podendo sob qualquer pretexto divulgar, revelar, reproduzir, utilizar ou dar conhecimento a terceiros, sob pena de rescisão deste instrumento e, ainda, de serem obrigadas a responderem, eventualmente, pela responsabilidade civil e penal advinda da divulgação de informações sigilosas. A obrigação de confidencialidade deverá ser cumprida do início da vigência deste contrato até 05 (cinco) anos após o término da vigência ou da denúncia ou rescisão deste ajuste.

7.3 De igual forma, as partes concordam, salvo quando exigido por lei ou por ordem judicial, a não disponibilizar as informações confidenciais da outra parte, por qualquer meio, a terceiros, para qualquer finalidade, exceto para a implementação do presente contrato e observadas as demais disposições deste contrato e demais instrumentos que o integram.

7.4 As partes concordam e obrigam-se a providenciar todas as medidas para assegurarem que as informações confidenciais não sejam divulgadas ou distribuídas por seus empregados ou agentes, em violação aos dispositivos do presente instrumento, restringindo, obrigatoriamente, o acesso às citadas informações apenas daqueles funcionários designados para a consecução do objeto deste contrato.

7.5 A informação confidencial de uma das partes não inclui informação que:

7.5.1 seja ou se torne, no decorrer do prazo contratual, parte do domínio público, independente de ação ou omissão da outra parte;
7.5.2 embora de conhecimento legítimo da outra parte, anteriormente à revelação, não tenha sido obtida diretamente ou indiretamente da parte reveladora;
7.5.3 legitimamente revelada à outra parte por uma terceira pessoa sem restrição sobre a revelação; e,
7.5.4 seja independente desenvolvida pela outra parte.

Cláusula Oitava – Da Garantia da Execução

8.1 A CONTRATADA deverá prestar garantia de execução contratual, correspondente a 5% (cinco por cento) do valor _____ do contrato, no prazo de _____ dias, contados da data de assinatura deste contrato, nas seguintes modalidades:

a) Caução em Dinheiro;
b) Fiança Bancária, ou
c) Seguro Garantia.

8.2 Nos casos de contratação de mais de uma unidade ou lote, deverá ser apresentada 01 (uma) Garantia de Execução Contratual para cada Unidade ou Lote.

8.3 No caso de Garantia de Execução Contratual, na modalidade “Caução em Dinheiro”, deverá ser efetuada no ato da assinatura do contrato, mediante comprovante de depósito, conforme dados abaixo:

Banco do Brasil: 001
Agência: 3221-2
Conta Poupança: 104.321-8
Variação: 51
Empresa: Serviço Social da Indústria – SESI
CNPJ: 03.779.133/0001-04

Banco do Brasil: 001
Agência: 3221-2
Conta Poupança: 1155-X
Variação: 51
Empresa: Serviço Nacional de Aprendizagem Industrial – SENAI
CNPJ: 03.774.819/0001-02

8.4 A devolução ocorrerá em até 30 (trinta) dias corridos, após a conclusão dos serviços, devidamente atualizado pela remuneração da caderneta de poupança, no período em questão.

8.5 No caso de Garantia de Execução Contratual, na modalidade “Fiança Bancária”, esta deverá ser emitida por Instituição Financeira legalmente autorizada pelo Banco Central e apresentada no original ou meio eletrônico, com firma reconhecida e expressa renúncia aos benefícios dos artigos 827, 834, 835, 837, 838 e 839 do Código Civil, sendo o seu prazo de validade, no mínimo, igual ao prazo de vigência do contrato que será firmado pela participante selecionada.

8.6 No caso de Garantia de Execução Contratual na modalidade “Seguro Garantia”, a apólice deverá ser emitida por uma Companhia de Seguros legalmente autorizada pela SUSEP, apresentada no original ou meio eletrônico, sendo seu prazo de vigência, no mínimo, igual ao prazo de vigência do contrato, que será firmado pela participante selecionada.

8.7 Na hipótese de prorrogação no prazo de vigência, reajustes/alteração do valor contratual, inclusive nos casos de celebração de termos aditivos de acréscimos quantitativos e/ou qualitativos que aumente o valor do contrato, a Contratada se obriga a complementar a garantia oferecida, para adequá-la ao valor atualizado do contrato.

Cláusula Nona – Do Acordo de Nível de Serviço

9.1. A CONTRATADA deverá assegurar os níveis de serviço relativos à disponibilidade da solução, ao atendimento e à resolução de incidentes, ao suporte técnico e à substituição de equipamentos, conforme os parâmetros estabelecidos no Memorial Descritivo referente ao PSDA nº 494/2026 e em seus respectivos anexos.

9.2. A solução deverá apresentar disponibilidade mínima de 99,99% (noventa e nove vírgula noventa e nove por cento), considerando o funcionamento ininterrupto (24x7x365) do cluster, observados os critérios de apuração estabelecidos no Memorial Descritivo e em seus anexos.

9.3. O atendimento aos incidentes deverá observar os prazos máximos de resposta, início da resolução e resolução ou disponibilização de solução de contorno, conforme a classificação de severidade prevista no Memorial Descritivo.

9.4. A CONTRATADA deverá disponibilizar suporte técnico especializado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o ano, em português, bem como assegurar a substituição de hardware nos prazos contratados, observada a cobertura do serviço FortiCare.

9.5. A disponibilidade da solução será apurada mensalmente, considerando o funcionamento ininterrupto (24x7x365) do cluster, com consolidação anual dos resultados.

9.6 O descumprimento dos níveis de disponibilidade estabelecidos sujeitará a CONTRATADA à aplicação de glosa sobre a remuneração mensal dos serviços continuados e do suporte técnico, excluídos os valores correspondentes aos ativos de hardware e às licenças perpétuas, observados os seguintes percentuais, conforme o índice de disponibilidade apurado no respectivo mês:

I – 2% (dois por cento), para disponibilidade igual ou superior a 99,90% e inferior a 99,99%;
II – 5% (cinco por cento), para disponibilidade igual ou superior a 99,00% e inferior a 99,90%;
III – 10% (dez por cento), para disponibilidade inferior a 99,00%.

9.7. A glosa será calculada mensalmente sobre o valor da remuneração dos serviços continuados e do suporte técnico correspondente ao respectivo mês, excluídos os valores dos ativos de hardware e das licenças perpétuas. A soma das glosas e dos demais descontos decorrentes do descumprimento dos níveis de serviço previstos neste contrato ficará limitada a 30% (trinta por cento) da referida base de cálculo mensal.

9.8 A CONTRATADA será comunicada acerca da apuração da disponibilidade e da glosa proposta, podendo apresentar manifestação fundamentada e documentos comprobatórios no prazo estabelecido pelo SESI-SP e SENAI-SP, antes da efetivação da glosa. A manifestação será analisada pelo SESI-SP e SENAI-SP, que comunicarão à CONTRATADA a decisão adotada.

9.9 A aplicação de glosas por 3 (três) meses consecutivos poderá ensejar a rescisão do contrato, observados o procedimento contratual aplicável e as demais medidas cabíveis.

Cláusula Décima – Da Subcontratação

10.1. É vedada a subcontratação, total ou parcial, do objeto deste contrato, cabendo exclusivamente à CONTRATADA a responsabilidade pela execução integral das obrigações assumidas.

Cláusula Décima Primeira – Da Proteção de Dados

11.1 As Partes declaram que cumprirão a Lei Geral de Proteção de Dados (“LGPD”) nº 13.709, de 14 de agosto de 2018 e todas as demais leis, normas e regulamentos aplicáveis, assim como cumprirão suas respectivas atualizações e atenderão os padrões aplicáveis em seu segmento em relação ao tratamento de dados pessoais, tanto no que diz respeito aos dados pessoais disponibilizados de uma Parte à outra Parte, pelo que se segue:

a) Possuem todos os direitos, consentimentos e/ou autorizações necessários exigidos pela LGPD, e demais leis aplicáveis, para divulgar, compartilhar e/ou autorizar o tratamento dos dados pessoais para o cumprimento de suas obrigações contratuais e/ou legais;

b) Não conservarão dados pessoais que excedam as finalidades previstas no Contrato e seus anexos;

c) Informarão e instruirão os seus colaboradores, prestadores de serviços e/ou terceiros sobre o tratamento dos dados pessoais, observando todas as condições desse Contrato, inclusive na hipótese de os titulares de dados terem acesso direto a qualquer sistema (*online* ou não) para preenchimento de informações que possam conter os dados pessoais, garantindo a privacidade e confidencialidade dos dados pessoais, e mantendo um controle rigoroso sobre o acesso aos dados pessoais;

d) Não fornecerão ou compartilharão, em qualquer hipótese, dados pessoais sensíveis de seus colaboradores, prestadores de serviços e/ou terceiros, salvo se expressamente solicitado por uma Parte à outra, caso o objeto do Contrato justifique o recebimento de tais dados pessoais sensíveis, estritamente para fins de atendimento de legislação aplicável;

e) Informarão uma Parte à outra sobre qualquer incidente de segurança, relacionado ao presente instrumento, por quaisquer meios, do respectivo incidente;

f) Se for o caso, quando deter dados pessoais, irão alterar, corrigir, apagar, dar acesso, anonimizar ou realizar a portabilidade para terceiros de dados pessoais, mediante solicitação da Parte requerente;

g) Excluirão, de forma irreversível, os dados pessoais retidos em seus registros, mediante solicitação da outra Parte ou dos titulares dos dados, a qualquer momento, salvo conforme determinado por lei ou ordem judicial;

h) Implementarão, quando for o caso, medidas de segurança substanciais, de acordo com os padrões aplicáveis na indústria projetados para garantir a segurança, confidencialidade e integridade dos Dados Pessoais;

i) Colaborarão com a outra Parte, mediante solicitação desta, no cumprimento das obrigações de responder a solicitações e reivindicações de pessoa e/ou autoridade governamental, a respeito de Dados Pessoais;

j) Ao término do Contrato cessará o tratamento, inclusive qualquer uso dos Dados Pessoais e devolverá à outra Parte ou destruirá todos os Dados Pessoais e todas as cópias destes, exceto se obrigada a manter cópia de determinados Dados Pessoais estritamente em virtude de lei ou de ordem judicial;

k) O tratamento dos dados coletados, somente quando autorizados, de uma Parte à outra, poderão ser conservados pelo período de 5 (cinco) anos após o término do presente instrumento, com sua posterior eliminação, sendo autorizada sua conservação nas hipóteses descritas no artigo 16 da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018);

l) Assegurarão que colaboradores, prestadores de serviços, terceiros, parceiros e membros da equipe técnica que venham a ter acesso aos dados durante o desenvolvimento do projeto cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais, nunca cedendo ou divulgando tais dados a terceiros, salvo se expressamente autorizado pelo titular, por força de lei ou determinação judicial;

m) As Partes não poderão subcontratar nem delegar o Tratamento dos Dados Pessoais sem o consentimento prévio por escrito da outra Parte, mas podem as Partes preservar e conservar os dados por si ou por empresa contratada especialmente para este fim durante a vigência do presente Contrato; e

n) As Partes declaram ciência de que os dados fornecidos, uma vez anonimizados, não são considerados Dados Pessoais, como estabelece o artigo 12 da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

11.2 Independentemente do disposto em qualquer outra cláusula deste Contrato, ou se for o caso do Contrato original e eventuais aditivos, a CONTRATADA é a única responsável por todo e qualquer dano decorrente do descumprimento da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção dos Dados, pela CONTRATADA, por seus colaboradores, prepostos, subcontratados, parceiros comerciais, empresas afiliadas ou qualquer agente ou terceiro a ela vinculado ou que atue em seu nome.

11.3 A CONTRATADA deverá cientificar formalmente os seus funcionários, alocados nos postos de trabalho do SESI-SP e do SENAI-SP, por meio da inclusão de cláusula nos respectivos contratos de trabalho e/ou outro instrumento específico, de que o SESI-SP e o SENAI-SP, por si ou por meio de empresa especializada por ela contratada, terão acesso e efetuarão o tratamento, compartilhamento e guarda dos dados pessoais e pessoais sensíveis desses por até 05 (cinco) anos após o término da vigência do contrato de prestação de serviços, por força legal e contratual, nos termos da Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018).

Cláusula Décima Segunda – Da Denúncia

12.1 O presente contrato poderá ser denunciado por qualquer das partes, mediante comunicação à outra parte com antecedência mínima de 60 (sessenta) dias.

12.2 Na hipótese de denúncia pela CONTRATADA, ou de extinção antecipada por fato a ela imputável, a CONTRATADA deverá restituir ao SESI-SP e ao SENAI-SP, proporcionalmente ao período remanescente, os valores recebidos por obrigações de suporte, níveis de serviço e demais prestações continuadas ainda não executadas, sem prejuízo da manutenção das licenças e subscrições já registradas em nome das Entidades.

Cláusula Décima Terceira – Da Rescisão

13.1 O presente contrato poderá ser rescindido em caso de descumprimento de quaisquer de suas cláusulas contratuais, arcando a parte que der motivo, com o pagamento à parte inocente, da multa contratual prevista neste instrumento, caso a parte inadimplente, após notificada, não adimplir com sua obrigação no prazo de 03 (três) dias corridos a partir do recebimento da notificação.

13.2 Por iniciativa motivada do SESI-SP e do SENAI-SP, o contrato ainda poderá ser rescindido:

a) pela infração a qualquer cláusula do presente contrato;
b) se a CONTRATADA paralisar o serviço por ____ dias, sem motivo justificado;
c) em caso de recuperação judicial/extrajudicial, falência, dissolução ou liquidação da CONTRATADA;
d) na hipótese de suspensão dos serviços por determinação de autoridades competentes, ficando a CONTRATADA responsável pelos eventuais aumentos nos custos de serviços e pelas perdas e danos que o SESI-SP e o SENAI-SP venham a sofrer;
e) decorrente de associação com outrem, fusão ou incorporação da CONTRATADA, ou ainda alteração de seu Contrato Social ou Estatuto, que modifique seu objeto, estrutura ou prejudique a execução deste contrato;
f) pela subcontratação total, cessão ou transferência do contrato;

g) em caso de subcontratação parcial dos serviços, sem prévia concordância do SESI-SP e do SENAI-SP; e
h) cometimento reiterado de faltas ou não atendimento das determinações da fiscalização do SESI-SP e do SENAI-SP.

Cláusula Décima Quarta – Das Condições Gerais

14.1 A CONTRATADA é a única e exclusiva responsável por quaisquer danos ou prejuízos, que eventualmente possa causar a terceiros, bem como seus prepostos e empregados, em decorrência da execução dos serviços objeto do presente ajuste, sem que possa ser imputada qualquer responsabilidade ou ônus ao SESI-SP e ao SENAI-SP pelos ressarcimentos ou indenizações devidos.

14.2 Na hipótese do SESI-SP e o SENAI-SP, por meio da Gerência responsável, virem a exigir a comprovação do cumprimento de todas as obrigações legais a que se sujeita a CONTRATADA, tal comprovação deverá ser realizada mediante a apresentação dos documentos, demonstrando que se encontra em dia com todos os recolhimentos, conforme for o caso, dos tributos, contribuições, taxas, encargos trabalhistas e previdenciários, e de demais documentos legais que o SESI-SP e o SENAI-SP, a seu exclusivo critério, entendam ser necessários.

14.3 O SESI-SP e o SENAI-SP não serão responsáveis, seja a que título for, por quaisquer perdas, danos, extravios ou desaparecimento de objetos pertencentes à CONTRATADA ou aos membros da sua equipe.

14.4 Caso a CONTRATADA não apresente ou apresente a documentação incompleta solicitada pelo SESI-SP e pelo SENAI-SP, tal fato ensejará a imediata suspensão do pagamento de qualquer valor, que somente será efetuado mediante a regularização da falta, sem prejuízo do presente instrumento ser rescindido pelo SESI-SP e pelo SENAI-SP por inadimplemento contratual por parte da CONTRATADA, com pagamento da multa contratual aqui estipulada e apuração de perdas e danos.

14.5 Fica estabelecido que o SESI-SP e o SENAI-SP não responderão, sob qualquer hipótese, pelos ônus decorrentes do uso indevido de equipamentos, programas de computador e demais ferramentas e recursos auxiliares protegidos nos termos da lei, que a CONTRATADA tenha violado na execução dos serviços objeto deste instrumento, cabendo à mesma CONTRATADA responder, civil e penalmente, por eventuais infrações cometidas.

14.6 Na assinatura do contrato a CONTRATADA toma ciência da Política de Segurança da Informação do SESI-SP e do SENAI-SP, firmando o documento Termo de Confidencialidade, conforme destacado na Cláusula Sétima, cujo conteúdo deverá ser divulgado a todos os seus profissionais que integrarão a equipe de prestação de serviços do SESI-SP e do SENAI-SP, de maneira que os termos ali consignados sejam efetivamente conhecidos e adotados.

14.7 Qualquer tolerância no cumprimento do presente instrumento será entendida como mera liberalidade das partes e não como novação, que não se presumirá em nenhuma hipótese, configurando-se apenas por escrito e firmada por ambas as Partes.

14.8 As Partes cumprirão integralmente, a todo tempo, de acordo com a Lei Anticorrupção Brasileira (Lei nº 12.846/2013), bem como com todas as outras leis antissuborno, anticorrupção, sobre conflitos de interesse ou outras leis, normas ou regulamentos com finalidade e efeito semelhantes aplicáveis à CONTRATADA ou ao SESI-SP e ao SENAI-SP.

14.9 Se durante a vigência do presente contrato, o SESI-SP e o SENAI-SP, forem obrigados, por Lei ou Ato de Autoridade Pública, a interromper as atividades que constituem o objeto deste contrato, o mesmo poderá ser (extinto) rescindido, independentemente do pagamento da multa ou qualquer outra verba, seja a que título for.

14.10 Se durante a vigência do presente contrato ocorrer motivos de caso fortuito e/ou de força maior que impeça a continuidade da execução do contrato, tais como calamidades públicas, estado de emergência, que gerem impacto de forma a restringir circulação de pessoas por medida de segurança pública, motivos de interesse público e/ou bem estar social, declarado/s ou não por Autoridade/s, Comunicado/s emitido/s pela Organização Mundial da Saúde ou Organismos Governamentais, poderá ocorrer a suspensão do presente instrumento, e se for o caso, com o cancelamento de cronogramas definidos, até o seu regular retorno, sem que haja qualquer penalidade, custo e despesa, a quaisquer das Partes, seja a que título for.

14.11 Fica estabelecido que a CONTRATADA é considerada, para todos os fins e efeitos jurídicos, como única e exclusiva empregadora dos profissionais alocados na prestação de serviço, sendo a responsável pelo cumprimento das obrigações trabalhistas e previdenciárias, cabendo-lhe reembolsar o SESI-SP e o SENAI-SP ou suas subsidiárias de todas as despesas que estes tiverem, inclusive custas, emolumentos e honorários advocatícios, resultantes de sua condenação judicial a honrar obrigações trabalhistas ou previdenciárias, ou ainda a pagar indenizações decorrentes das relações de trabalho.

14.12 O SESI-SP e o SENAI-SP poderão rejeitar os serviços que não satisfaçam os padrões exigidos nas especificações, sendo informado por escrito à CONTRATADA o motivo da rejeição.

14.13 O SESI-SP e o SENAI-SP reservam-se o direito de determinar o dia e horário para a execução das atividades de implementação, configuração ou manutenção da solução, inclusive fora do horário comercial padrão (08h às 18h) ou em finais de semana e feriados, desde que haja comunicação prévia à CONTRATADA com antecedência mínima de 24 (vinte e quatro) horas.

14.14 A CONTRATADA compromete-se a atender às solicitações dentro desse prazo, assegurando a disponibilidade de equipe técnica capacitada e recursos necessários para a execução segura e eficiente dos serviços, sem ônus adicional ao SESI-SP/SENAI-SP.

14.15 O acesso da CONTRATADA às instalações, ambientes, equipamentos ou sistemas do SESI-SP e do SENAI-SP deverá ocorrer de forma autorizada, controlada e compatível com a finalidade da execução dos serviços, não implicando acesso irrestrito a ambientes internos, sistemas corporativos ou ativos que não estejam diretamente relacionados ao objeto contratado.

Cláusula Décima Quinta – Das Penalidades

15.1 Atrasos e/ou descumprimento de quaisquer obrigações pactuadas neste instrumento e demais obrigações constantes do PSDA nº 494/2026, acarretará a aplicação de multa no percentual de 2% (dois por cento) do valor do contrato.

15.2 A parte que der motivo à rescisão ou por descumprimento das cláusulas e condições pactuadas, ou ainda, após a entrega, restar provado que os serviços/materiais e/ou equipamentos não atenderam as especificações, incorrerá no pagamento, à parte inocente, da multa equivalente a 10% (dez por cento) do valor total do contrato, ressalvado o direito ao credor de exigir indenização por prejuízo excedente, nos termos do parágrafo único do art. 416 do Código Civil.

15.3 O inadimplemento total ou parcial das obrigações contratuais assumidas pela CONTRATADA, dará ao SESI-SP e ao SENAI-SP o direito de rescindir unilateralmente o contrato, sem prejuízo de outras penalidades previstas, inclusive a de suspensão do direito de participar de processos de seleção junto ao SESI-SP e ao SENAI-SP por prazo não superior a 05 (cinco) anos, impedimento esse extensivo às pessoas físicas que constituíram a pessoa jurídica, as quais permanecem impedidas de participar enquanto perdurarem as causas da penalidade, independentemente de nova pessoa jurídica que vierem a constituir ou de outra em que figurem como sócios, e às pessoas jurídicas que tenham sócios comuns com as pessoas físicas acima mencionadas.

15.4 As penalidades previstas neste Contrato e no Memorial Descritivo são independentes, não excludentes e poderão ser aplicadas cumulativamente.

15.5 Os valores relativos às multas aplicadas, bem como outros valores que forem devidos pela CONTRATADA, poderão ser deduzidos dos créditos que possuir junto ao SESI-SP e ao SENAI-SP ou cobrados administrativa ou judicialmente.

Cláusula Décima Sexta – Da Reforma Tributária

16.1 À contratação aplicam-se as regras da Reforma Tributária (EC nº 132/2023 e LC nº 214/2025), sendo vedado o repasse unilateral de tributos, incluindo quaisquer encargos ou majorações de preços decorrentes da alteração legislativa.

16.1.1 Considera-se "Reforma Tributária" qualquer alteração na legislação tributária aplicável, incluindo, mas não se limitando a mudanças nas alíquotas, bases de cálculo, criação, extinção ou substituição de tributos, que venha a afetar os serviços objeto desta contratação.

16.2 A CONTRATADA declara ciência de que, até a completa implementação da Reforma Tributária, coexistirão quando aplicável, os atuais tributos incidentes sobre serviços (ISS, PIS, COFINS, CSLL, IRRF, INSS, entre outros) e os novos tributos (CBS – Contribuição sobre Bens e Serviços e IBS – Imposto sobre Bens e Serviços), cabendo-lhe integral responsabilidade pelo correto enquadramento, apuração, recolhimento e comprovação do pagamento dos tributos incidentes sobre a prestação do objeto desta contratação.

16.3 É vedado, à CONTRATADA, repassar, ao SESI-SP e ao SENAI-SP, de forma unilateral, quaisquer encargos tributários ou majorações de preços decorrentes da Reforma Tributária.

16.4 É vedado, à CONTRATADA, promover qualquer reajuste de preços com fundamento em alteração tributária sem prévia comprovação documental oficial da majoração da carga tributária incidente diretamente sobre o objeto desta contratação, devendo tal situação ser analisada em boa-fé pelas Partes e, se necessário, formalizado por documento assinado pela CONTRATADA e pelo SESI-SP e SENAI-SP, os quais reservam-se ao direito de auditar os cálculos apresentados.

16.5 Toda e qualquer nota fiscal de serviços deverá ser emitida em conformidade com o padrão nacional de NFS-e, atendendo às exigências legais vigentes, inclusive quanto à discriminação das alíquotas e bases de cálculo de ISS, IBS e CBS. Notas fiscais emitidas de forma incorreta ou que não permitam a identificação clara dos tributos incidentes serão consideradas não recebidas, não gerando obrigação de pagamento até sua regularização.

16.6 Caso o SESI-SP e o SENAI-SP venham a sofrer autuação, multa, cobrança ou qualquer exigência fiscal decorrente de erro, omissão, classificação incorreta ou descumprimento das normas tributárias pela CONTRATADA, esta se compromete a assumir integralmente a

responsabilidade, isentando e indenizando o SESI-SP e o SENAI-SP por todos os valores, custos, honorários advocatícios e encargos que venham a ser despendidos.

16.7 As partes reconhecem que a eventual instituição de regimes de retenção tributária obrigatória (inclusive sobre IBS e CBS) será automaticamente aplicada à presente contratação, sem necessidade de aditamento, autorizando o SESI-SP e o SENAI-SP a procederem às retenções devidas e comprovar à CONTRATADA o recolhimento.

16.8 Em caso de alteração legislativa superveniente que modifique substancialmente a sistemática de incidência de tributos, as Partes comprometem-se a revisar este documento em boa-fé, buscando entendimento, vedada a suspensão dos serviços ou a exigência de valores adicionais pela CONTRATADA, sem prévia concordância do SESI-SP e do SENAI-SP, por meio de documento contratual.

Cláusula Décima Sétima – Da Representação da CONTRATADA

A CONTRATADA declara neste ato, para todos os fins e efeitos de direito, que o(s) signatário(s) é(são) seu(s) legítimo(s) representante(s) na data de assinatura deste instrumento, conforme documentos societários e quando for o caso, procuração, constantes de seu cadastro junto ao SESI-SP e ao SENAI-SP, estando ciente de que a falsidade na prestação desta informação, sem prejuízo de serem aplicadas as penalidades previstas neste instrumento, inclusive sua rescisão e apuração de perdas e danos, sujeitará todas as pessoas que para ela concorrerem, às penalidades previstas na legislação criminal relativas à falsidade ideológica (art. 299 do Código Penal).

Cláusula Décima Oitava – Da Assinatura Eletrônica

18.1 Quando for o caso, como alternativa à assinatura física, as Partes declaram e concordam que a assinatura deste Instrumento e todos os seus aditivos e afins poderá ser realizada eletronicamente.

18.2 As Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Instrumento, de acordo com o art. 219 do Código Civil, em formato eletrônico e assinado pelas Partes por meio de certificados eletrônicos, nos termos do art. 10, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (“MP 2.200-2”), declarando, desde já, plena anuência com a aposição das assinaturas eletrônicas neste Contrato na plataforma a ser definida pelas Partes.

18.3 Adicionalmente, as Partes signatárias deste Instrumento expressamente anuem, autorizam, aceitam e reconhecem como válida qualquer forma de comprovação da autoria de suas respectivas assinaturas por meio de certificados eletrônicos, nos termos da MP 2.200-2, de 24/08/2001, sendo certo que quaisquer de tais certificados será suficiente para comprovar a veracidade, autenticidade, integridade, validade e eficácia deste Contrato e seus termos, bem como a respectiva vinculação das Partes às suas disposições, nos termos dos artigos 441 e 784, III, do Código de Processo Civil.

Cláusula Décima Nona – Gestão e Fiscalização

Os serviços inerentes ao presente contrato serão conduzidos sob a gestão da Gerência Sênior de Tecnologia da Informação do SESI-SP e do SENAI-SP, que indicará funcionário(s) para exercer (em) a função de fiscal (is) do contrato, cumprindo verificar os documentos e relatórios relacionados aos serviços elaborados pela CONTRATADA, acompanhar a execução, as etapas e prazos determinados, averiguar e homologar os serviços prestados, bem como conferir, controlar e liberar

os valores constantes dos documentos de cobrança, além das demais atribuições previstas neste instrumento.

Cláusula Vigésima – Do Foro

As Partes elegem o foro da Comarca da Capital do Estado de São Paulo para dirimir eventuais dúvidas oriundas do presente contrato.

E, por estarem assim justas e contratadas, firmam o presente instrumento eletronicamente, considerando-se celebrado na data da última assinatura digital lançada pelas partes.

São Paulo, data da última assinatura digital.

SERVIÇO SOCIAL DA INDÚSTRIA – SESI
SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL – SENAI
Departamentos Regionais de São Paulo

Glauber Magalhães de Souza
Gerente Sênior de Tecnologia da Informação

CONTRATADA

_____
Nome:
CPF:
Cargo:

Testemunhas:

_____
Nome:
RG:

_____
Nome:
RG:

ANEXO E

REQUISITOS DA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Requisitos de Segurança da Informação

1.1. As disposições abaixo são aplicáveis a qualquer objeto de contratação, onde são fornecidos serviços, sistemas, plataformas de trabalho ou qualquer outro objeto que faça uso ou seja viabilizado através de meios tecnológicos e/ou computacionais.

1.2. A aplicação dos itens deve ser avaliada diante do contexto de fornecimento e requisitos do objeto descrito na minuta de edital, descartando-se requisitos deste que não sejam pertinentes ou associados ao objeto hora contratado.

1.3. Motivada pela evolução das ameaças e riscos à Segurança da informação e Privacidade, a CONTRATANTE poderá apresentar novos requisitos de segurança durante o fornecimento do objeto contratado ou serviço prestado, trazendo a razoabilidade como fundamento para esta adequação.

1.4. **Segurança na camada da aplicação**

1.4.1. A plataforma deverá conter Termo de Uso de Usuário Final, contendo as informações sobre os serviços prestados, condições de uso, privacidade, coleta e processamento de dados pessoais e sensíveis, refletindo diretrizes definidas pelo SESI-SP E SENAI-SP.

1.4.2. O sistema deverá possuir processo de exclusão dos dados (pessoais ou sensíveis) coletados a pedido do cliente e em alinhamento com regras estabelecidas pelo SESI-SP E SENAI-SP. Ressalvo nos casos que a lei exige a guarda obrigatória.

1.4.3. A arquitetura de sistema deverá ser concebida ao menos em duas camadas, separando a camada de dados da camada de front-end. A camada de front-end é entregue de modo que o usuário não consiga identificarem qual linguagem o sistema foi desenvolvido.

1.4.4. Deverá ser feita sanitização de entrada de dados em todos os campos. O código deverá ser escrito conforme melhores práticas da OWASP (Open Web Application Security Project).

1.4.5. A aplicação deverá registrar informações sobre quem se conectou na aplicação, bem como quem fez o que e quando. Os registros deverão ser armazenados por 6 meses. Quem (Credencial e IP), quando (dia/hora/minutos padrão UTC), o que foi acessado (sistema/banco/tabela/registro) e o tipo de transação (remoção/modificação/leitura)."

1.4.6. A aplicação deverá possibilitar a implantação de políticas de senha, conforme seguem:

a) Após 5 (cinco) tentativas inválidas de autenticação nos sistemas, o perfil deve ser bloqueado.
b) A reutilização de senhas obedecerá ao ciclo mínimo de 2(duas) trocas, ou seja, as últimas duas senhas não poderão ser reutilizadas.

c) As senhas deverão ter no mínimo 8 dígitos.
d) Na criação ou troca de senhas, devem ser adotadas senhas fortes.
e) A aplicação deverá possuir mecanismo de duplo fator e autenticação, compatível com o Office 365.

1.4.7. O sistema deverá possuir a capacidade de enviar e-mail “SMTP Relay”, contemplando mecanismo de autenticação.

1.4.8. Os sistemas deverão funcionar sem a necessidade do parent path habilitado.

1.4.9. O sistema não deverá possuir “Maintenance Hook”.

1.5. Requisitos gerais de Segurança da Informação para Provedor de Nuvem

1.5.1. Caso a solução seja hospedada em provedores de nuvem, os envolvidos deverão no mínimo, possuir as certificações de conformidade com as seguintes normas:

a) ISO 27.017 - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27.002 para serviços em nuvem.
b) ISO 27.018 - Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII.

1.6. Hospedagem das aplicações em Nuvem ou Datacenter

1.6.1. O provedor de Nuvem ou Datacenter não deverá hospedar dados em países cujo acesso aos mesmos pode ser feito pelo governo local sem a necessidade de autorização do proprietário ou mandado judicial.

1.6.2. No contrato de prestação de serviços não poderá conter uma cláusula apontando o provedor de Nuvem ou Datacenter como dono da informação.

1.6.3. Somente poderão ser contratados provedores de nuvens cujo contrato especifique foro Brasileiro para resolução de questões judiciais.

1.6.4. O provedor de Nuvem ou Datacenter deve ter certificações reconhecidas no mercado que ateste suas premissas básicas de segurança: climatização, controle de acesso, sistema de combate ao incêndio a gás F-200, cabeamento estruturado, instalações e proteções elétricas adequadas e demais boas práticas de mercado.

1.6.5. O provedor de serviço de Nuvem ou Datacenter deverá utilizar ferramenta de backup, que possibilite a implementação da política de retenção abaixo, bem como o download de todos os dados nela armazenados. Política de retenção:

a) Diário: últimos 5 dias;
b) Semanal: últimas 5 semanas;
c) Mensal: últimos 12 meses;
d) Anual: últimos 5 anos.

1.6.6. O provedor de Nuvem ou Datacenter deverá possibilitar o controle e gerenciamento de portas de comunicação do protocolo de rede TCP/IP.

1.6.7. O provedor de Nuvem ou Datacenter deverá possuir serviço de Antivírus para os ativos de informação nas nuvens.

1.6.8. O provedor de Nuvem ou Datacenter deverá possuir serviço de IPS (Intrusion Prevention System) para os ativos de informação nas nuvens.

1.6.9. O provedor de Nuvem ou Datacenter deverá possuir serviço de WAF (Web Application Firewall) baseado no padrão OASP versão 1, 2 e 3 para os ativos de informação nas nuvens.

1.6.10. O provedor de Nuvem ou Datacenter deverá possuir serviço contra-ataques de negação de serviço distribuído.

1.6.11. O provedor do serviço de Nuvem ou Datacenter deverá apresentar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.

1.6.12. Somente responsável pela implantação, administração ou seus superiores, indicados pelo SESI-SP E SENAI-SP, poderão autorizar a inclusão de uma conta com “privilégios administrativos” na plataforma.

1.6.13. A plataforma deverá permitir ao SESI-SP E SENAI-SP a utilização de scanner de vulnerabilidade não intrusivo, tendo como principal objetivo identificação vulnerabilidades na aplicação.

1.6.14. A plataforma deverá disponibilizar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.

1.6.15. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos da informação imprescindíveis ao pleno desempenho de suas atividades.

1.7. Direitos de Propriedade da Base de Dados

1.7.1. Toda informação gerada ou transformada pelas Contratantes nos recursos computacionais da Contratada é de propriedade única e exclusiva do SESI-SP E SENAI-SP.

1.7.2. No encerramento do contrato a Contratada deverá entregar todas as informações de propriedade das Contratantes em meio eletrônico, em formato a ser definido pelo SESI-SP E SENAI-SP, tais como scripts, configurações, procedimentos, relatórios de melhoria de serviço e acompanhamento de ações realizadas na vigência do contrato, de modo a permitir a correta migração dos serviços para outro ambiente de infraestrutura de Cloud Computing.

1.7.3. Toda a base de dados de soluções de Atendimento Técnico, contendo todos os históricos e procedimentos deverão ser disponibilizados pela Contratada às Contratantes em formato padrão e com a sua estrutura de dados.

1.7.4. Ao término do contrato todos os dados deverão ser excluídos, das plataformas da Contratada.

1.8. Sigilo das Informações

1.8.1. Guardar sigilo dos dados a que tiver acesso ou que vierem a ser compartilhados, bem como sobre os produtos de propriedade das Contratantes, além daqueles processados e gerados no ambiente físico da Contratada, reconhecendo serem estes de propriedade exclusiva do SESI-SP E SENAI-SP, os quais não podem ser cedidos, copiados, reproduzidos, publicados, divulgados de nenhuma forma, nem colocados à disposição direta ou indiretamente, locados ou vendidos a terceiros, mesmo após o encerramento do contrato, consoante o quanto contido no Termo de Confidencialidade a ser firmado pelas partes em conjunto com o instrumento contratual;

1.8.2. Não utilizar a marca das Contratantes ou qualquer material desenvolvido pelo SESI-SP E SENAI-SP para seus produtos e programas, assim como os dados dos clientes a que tenha acesso no decorrer das atividades inerentes ao contrato, em ações desenvolvidas pela Contratada fora do âmbito de atuação do contrato;

1.8.3. Tratar em caráter de estrita confidencialidade todas as informações a que tenha acesso em função do contrato, agindo com diligência para evitar sua divulgação verbal ou escrita, ou permitir o acesso, seja por ação ou omissão, a qualquer terceiro;

1.8.4. Manter, por si, por seus prepostos e contratados, irrestrito e total sigilo sobre quaisquer dados que lhe sejam fornecidos em decorrência do contrato.

1.8.5. Todas as informações veiculadas e armazenadas e/ou trafegadas nos recursos computacionais envolvidos na presente contratação, devem ser tratadas com absoluta reserva em qualquer condição e não podem ser divulgadas ou dadas a conhecer a terceiros não autorizados, aí se incluindo os próprios funcionários, estagiários, terceiros ou parceiros das Contratantes, sem a autorização destes.

1.9. Requisitos Gerais de Segurança da Informação

1.9.1. A Contratada deverá, juntamente com seu projeto de implantação, apresentar ao SESI-SP E SENAI-SP documento contendo sua Política de Segurança da Informação conforme solicitado a seguir.

1.9.2. A Política de Segurança da Informação da Contratada deverá estar alinhada com aquela adotada pelas Contratantes e abordar no mínimo os aspectos relacionados abaixo:

a) Responsabilidades associadas a acesso, gestão e guarda de informações, estabelecidas para os profissionais integrantes dos seus quadros ou terceiros;

b) Cumprimento irrestrito da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18) e possuir conformidade com a GDPR (General Data Protection Regulation);
c) Sempre que possível, recomendado ou solicitado pela contratante, implementar o uso de criptografia e/ou certificados digitais para operação ou gerenciamento do ambiente;
d) Emprego de equipamento de firewall, em suas instalações, com suporte a VPN/IPSEC, utilizando apenas algoritmos criptográficos classificados como "uso aceitável" pelo NIST (National Institute of Standard Technology), definindo as fronteiras físicas e lógicas entre as redes das Contratantes e da Contratada e outros acessos necessários à prestação dos serviços, bem como solução de software de prevenção de intrusão (IPS) para o ambiente;
e) Utilização de softwares antivírus e de proteção a ameaças avançadas, em todos os equipamentos das suas instalações, capazes de detectar e remover vírus, cavalos de troia, warms e ameaças correlatas, com atualizações frequentes e automáticas das vacinas e novas versões contemplando todos os servidores e estações de rede. Essa solução deverá ter capacidade e performance compatível com aquela instalada e em operação no ambiente das Contratantes;
f) A Contratada deverá permitir às Contratantes o acesso local ou remoto aos seus sistemas, assim como a todo e qualquer equipamento disponibilizado na prestação dos serviços, bem como aos ambientes físicos com controle de acesso, para fins de auditoria em segurança;
g) Deverão ser adotados procedimentos de acesso seguro ambiente, permitindo inclusive a autenticação forte e utilização de múltiplos fatores de autenticação, bem como a aplicação de certificados digitais e técnicas criptográficas para armazenamento de dados;

2 Requisitos de Privacidade e Conformidade LGPD

2.1 Os requisitos de privacidade sob perspectiva da Lei Geral de Proteção de Dados (LGPD – Lei 13.709/18), serão aplicáveis quando o objeto da contratação envolva direta ou indiretamente o tratamento de dados pessoais, especialmente os categorizados como sensíveis.

2.2 Qualquer item anterior presente neste anexo ou na minuta de edital que discorra sobre mesmo tema ou definição, deve ser interpretado de forma complementar com ênfase no entendimento de melhor garantia aos direitos dos titulares dos dados e/ou maior conformidade com a legislação aplicável.

2.3 Salvo disposições contrarias específicas, os termos abaixo terão as seguintes definições:

a) **Titulares:** Pessoa física singular identificada ou identificável, a qual poderá ter seus dados pessoais tratados;
b) **Dados Pessoais:** Qualquer informação relativa a uma pessoa singular identificada ou identificável ou qualquer outra informação que se qualifica como “Dados Pessoais” nos termos das leis de proteção de Dados.
c) **Dados Sensíveis:** Qualquer informação do titular que possa revelar sua origem racial ou étnica, religião, filiação sindical, opinião política, dados referentes à saúde e vida sexual, dados genético ou biométrico.

d) **Tratamento:** Qualquer operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

e) **Controlador:** Pessoas jurídica ou estabelecimento que nos termos da lei atua como controlador das informações, determinando as finalidades, meios de tratamento e demais ações sobre os dados pessoais sob sua responsabilidade.

f) **Operador:** Pessoa natural ou jurídica que sob orientação ou determinação do Controlador, executa o processamento e tratamento de dados pessoais dos titulares.

g) **Encarregado:** Pessoa nomeada nos termos da lei para atuar como canal de comunicação entre Controlador, Operadores, Titulares, Agências Reguladoras e demais interessados e responsáveis pela operacionalização e conformidade com a LGPD

2.4 Para efeito de delimitação de papeis e responsabilidades, neste documento a CONTRATANTE desempenhará o papel de CONTROLADOR e a CONTRATADA o papel de OPERADOR.

2.5 O OPERADOR deverá obter termo de confidencialidade dos seus colaboradores que estiverem envolvidos no tratamento dos dados em nome do CONTROLADOR, sendo esta exigência dispensada caso outro documento interno estabelecido tenha mesma aplicação e validade, por exemplo contrato de trabalho.

2.6 A OPERADOR deverá apresentar as informações do seu encarregado de proteção de dados, ou, colaborador que desempenhe atividades e responsabilidade semelhante sobre o tema, caso o OPERADOR seja dispensado de nomeação formal conforme previsão da LGPD.

2.7 O tratamento dos dados pessoais deverá ser executado de forma limitada e de acordo com as orientações e definições de finalidade determinados pelo CONTROLADOR.

2.8 De acordo com as instruções fornecidas pelo CONTROLADOR, o OPERADOR deve ajustar, excluir ou bloquear os dados processados, notificando sem atrasos se em sua opinião a instrução infringir as regulamentações aplicáveis de proteção de dados.

2.9 O OPERADOR deverá fornecer ao CONTROLADOR as informações necessárias para permitir que este cumpra as obrigações de notificação, mantenha registros das atividades de processamento e/ou realize a avaliação de impacto da proteção de dados caso necessário.

2.10 Os dados pessoais tratados deverão ser devolvidos ao CONTROLADOR e eliminados ao final do contrato ou sob sua solicitação, exceto em situações em que legislação especifique a necessidade e condição de manutenção dos dados.

2.11 Em caso de exclusão de dados por solicitação do CONTROLADOR, fica estabelecida a necessidade do OPERADOR demonstrar que os dados foram eliminados e não poderão ser reconstruídos, evidenciando inclusive por escrito que todos que todas as mídias foram devolvidas ou destruídas. Caso haja requisitos legais vinculativos que não permitam apagar dados contratuais ou categorias de dados, o OPERADOR deverá informar o CONTROLADOR sobre tais requisitos.

2.12 O OPERADOR deverá possuir Política de Segurança e Privacidade que exponha suas diretrizes e definições sobre o tema privacidade.

2.13 É vedado ao OPERADOR a subcontratação de operadores sem previa análise e expressa autorização do CONTROLADOR.

2.14 O OPERADOR deve estabelecer programa de Segurança da Informação e privacidade baseado nos principais Frameworks de mercado, como por exemplo ISO 27001/27002/27701, NIST etc., informando ao CONTROLADOR os dados para contato do seu gestor sobre o tema.

2.15 O programa de Segurança da Informação e Privacidade do OPERADOR deverá contar com ciclo de identificação e resposta à incidentes.

2.16 O OPERADOR deverá notificar qualquer incidente de segurança, tendo prazo de 72 horas para comunicar os que envolvam ou possam impactar dados pessoais tratados em nome do CONTROLADOR.

2.17 A critério do CONTROLADOR, deverão ser coordenadas medidas técnicas e organizacionais voltadas para Segurança da Informação e Privacidade, incluindo visitas às instalações do OPERADOR para auditorias e validação das medidas estabelecidas.

2.18 O CONTROLADOR ou seus representantes têm o direito de realizar verificações em cumprimento aos requisitos deste Contrato. O OPERADOR deve fornecer as informações desejadas e, mediante solicitação do CONTROLADOR e dentro de um prazo razoável, apresentar provas documentais de que cumpriu suas obrigações, preenchendo um questionário fornecido pelo CONTROLADOR ou confirmando por escrito que as medidas acordadas são adequadas e atuais.

2.19 O OPERADOR deve notificar o responsável pelo gerenciamento do contrato do CONTROLADOR por escrito, se houver alguma alteração significativa nas medidas técnicas e organizacionais descritas. No caso de qualquer redução previsível na efetividade da segurança, o consentimento do CONTROLADOR deve ser obtido por escrito antes que a alteração seja realizada.

2.20 O OPERADOR deverá implementar programa de treinamento e conscientização sobre Segurança da Informações e Privacidade, principalmente com temas e ações relacionadas privacidade e conformidade com a LGPD.

2.21 O OPERADOR deverá desenvolver, manter e apresentar relatório sobre brechas na segurança e proteção de dados, bem como inventário e ciclo de gestão de riscos em segurança da Informação.

O OPERADOR deve informar o CONTROLADOR sem demora sobre verificações das autoridades de supervisão que ocorrem na empresa do OPERADOR, ou na infraestrutura de TI utilizada, e onde os dados pessoais do CONTROLADOR estão sendo processados.

2.22 Na hipótese de iminente acesso aos dados do CONTROLADOR no contexto de apreensão, confisco, inquéritos judiciais ou outras ações aplicáveis por parte das autoridades, ou no contexto de procedimentos de insolvência ou outras medidas de terceiros, o OPERADOR deverá comunicar imediatamente tal situação ao CONTROLADOR.

2.23 O OPERADOR deverá informar sem demora a todas as partes envolvidas em tal ação que o poder de disposição sobre os dados sujeitos ao presente contrato está com o CONTROLADOR, não devendo transferir qualquer dado a terceiros nem permitir que terceiros tenham acesso aos dados sem a expressa autorização do CONTROLADOR.

2.24 O OPERADOR nos termos da Lei Geral de Proteção de Dados é solidário junto ao CONTROLADOR no desempenho das obrigações e cumprimento da legislação, devendo atuar ativamente para conformidade e pronta resposta.

ANEXO F

MINUTA DO TERMO DE CONFIDENCIALIDADE

SERVIÇO SOCIAL DA INDÚSTRIA – SESI
SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL - SENAI

Pelo presente instrumento e na melhor forma de direito, em que são partes, de um lado, o SERVIÇO SOCIAL DA INDÚSTRIA – SESI, Departamento Regional de São Paulo, inscrito no CNPJ sob o n.º 03.779.133/0001-04, doravante, simplesmente, denominado, SESI-SP e o SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL, Departamento Regional de São Paulo, inscrito no CNPJ sob o n.º 03.774.819/0001-02, doravante, simplesmente, denominado, SENAI-SP, com sede nesta Capital, na Avenida Paulista n.º 1313, 3º andar, Bairro Bela Vista, neste ato representado por seu ……, ……..; e, de outro lado, a …….., inscrita no CNPJ sob n° ……, com sede na Rua/Av. ……nº ….., Bairro ……. na cidade de ……., Estado de ……, aqui representada em conformidade com seus atos constitutivos e neste instrumento designada EMPRESA;

CONSIDERANDO que:

(a) a segurança e/ou proteção da informação é aqui caracterizada pela preservação da: CONFIDENCIALIDADE (garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso), INTEGRIDADE (salvaguarda da exatidão e completeza da informação e dos métodos de processamento), e DISPONIBILIDADE (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e,

(b) o SESI-SP e o SENAI-SP e a EMPRESA resolvem firmar o presente instrumento, doravante, denominado de “TERMO DE CONFIDENCIALIDADE”, que se regerá pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DAS INFORMAÇÕES CONFIDENCIAIS

1.1 São consideradas informações confidenciais, portanto, protegidas pelo presente Termo, todos os dados de natureza técnica, operacional, comercial, jurídica e financeira, bem como toda e qualquer informação que venha a ser “trocada” entre as partes, salvo aquelas cuja confidencialidade seja expressamente afastada.

1.2 A forma através da qual suceder a troca ou o acesso às informações classificadas é irrelevante para os efeitos deste acordo, sendo que os documentos impressos, manuscritos, *fac-símiles*, *laser-discs*, *pendrives*, disquetes ou qualquer outro meio onde estejam armazenados dados confidenciais, devem ser mantidos em local seguro (com acesso restrito) e destruídos ou devolvidos à proprietária da informação, após sua devida utilização, conforme orientação fornecida por esta última.

CLÁUSULA SEGUNDA - DAS OBRIGAÇÕES DA EMPRESA

2.1 A EMPRESA compromete-se por todos aqueles que por seu intermédio venham a tomar conhecimento de informações confidenciais do SESI-SP e do SENAI-SP, a manter o mais absoluto sigilo, limitando a utilização dos dados disponibilizados às estritas necessidades da negociação, contrato ou similar, não utilizando, em hipótese alguma, tais informações em proveito próprio ou alheio.

2.2. Fica a EMPRESA expressamente proibida de transferir a terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações classificadas a que tenha tido acesso, no território brasileiro ou no exterior, para nenhuma pessoa física ou jurídica e para nenhuma outra finalidade que não seja a consecução de seus objetivos conjuntos com o SESI-SP e com o SENAI-SP.

2.3. A EMPRESA se obriga a adotar todas as cautelas possíveis, no sentido de restringir o acesso às informações confidenciais em seu poder e impedir sua indevida divulgação ou utilização, valendo-se de ações destinadas a evitar o "vazamento" das informações classificadas.

2.4. As informações confidenciais que venham a ser confiadas à EMPRESA somente poderão ser repassadas aos administradores, prepostos e terceiros diretamente envolvidos no processo e cujo acesso seja indispensável para consecução da transação, negociação ou contratação em curso, sendo estes advertidos do caráter sigiloso das informações, e ficando a EMPRESA expressamente responsável em caso de quebra na integridade e sigilo destes dados.

2.5. É vedado à EMPRESA, em qualquer hipótese, manter em seu poder após sua utilização, documento ou qualquer outro meio onde as informações confidenciais do SESI-SP e do SENAI-SP estejam consignadas, ficando expressamente proibida a extração de cópias, reproduções, *backup* ou outro meio de armazenamento de dados.

2.6. A EMPRESA se compromete a contatar a proprietária da informação confidencial, caso eventualmente perceba a necessidade de repassar a terceiros, informação classificada, ainda que o repasse seja de apenas parte da informação, oportunidade em que deverá ser firmado, se for do interesse da proprietária, outro termo de confidencialidade obrigando a totalidade das partes.

2.7. A EMPRESA deverá comunicar o extravio, perda ou violação de qualquer informação confidencial, não ficando responsável nem sendo considerada violação ao presente acordo no caso da informação confidencial ser divulgada em razão de ato ou fato ao qual a EMPRESA ou qualquer de seus empregados, prepostos e/ou colaboradores que for divulgada em decorrência de fatos que tenham ocorrido em razão de caso fortuito e/ou força maior.

2.8. Se por decisão judicial a EMPRESA for obrigada a revelar informação ou dado que venha, ainda que indiretamente, a expor informação confidencial do SESI-SP, este deverá ser previamente comunicado.

2.9. Não serão consideradas informações confidenciais aquelas que sejam do prévio conhecimento da EMPRESA, de conhecimento público ou que venham a se tornar públicas por expressa vontade da proprietária da informação.

CLÁUSULA TERCEIRA - DAS INFORMAÇÕES CONJUGADAS

Na hipótese de surgirem informações relevantes da própria relação entre as partes, ou seja, se as informações confidenciais do SESI-SP e do SENAI-SP forem conjugadas com outros dados confidenciais da EMPRESA, estas serão consideradas informações classificadas de propriedade conjunta do SESI-SP e do SENAI-SP , sendo que sua divulgação e utilização somente sucederão mediante prévia e expressa autorização de ambas as partes.

CLÁUSULA QUARTA - DA UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

4.1. Nos precisos termos da cláusula primeira, o presente termo tem por objeto principal possibilitar à EMPRESA o acesso a informações confidenciais do SESI-SP, indispensáveis para a realização de negociação ou transação comercial, sem importar, contudo, em qualquer transferência ou cessão de informações.

4.2. As informações confidenciais são utilizáveis única e exclusivamente por seu proprietário, não autorizando o presente instrumento, seu uso pela EMPRESA, a não ser para a fiel execução de negociação, contrato ou qualquer outra transação que envolva o proprietário da informação.

4.3. Os direitos resultantes das informações confidenciais ou de seu emprego, bem como qualquer outro direito relativo à propriedade dessas informações também não se transferem através do presente.

CLÁUSULA QUINTA - DAS DISPOSIÇÔES GERAIS

5.1 Os empregados/prepostos da EMPRESA se comprometem a conhecer, observar e agir em conformidade com as Políticas de Segurança da Informação do SESI-SP e do SENAI-SP e/ou outras diretrizes, normas, instruções de trabalho e procedimentos relacionados, protegendo e preservando a integridade e confidencialidade de todos os dados e informações dos quais tome conhecimento ou utilize no exercício das suas funções, que serão tidos como sigilo profissional, inclusive após a cessação das suas atividades no SESI-SP e no SENAI-SP; estando cientes de que o desrespeito às diretrizes, normas e procedimentos relacionados com a segurança da informação e outras normas e procedimentos do SESI-SP e do SENAI-SP de que tenha sido dado conhecimento durante o exercício das suas funções, constitui *Violação de Segurança da Informação* e que, em caso de desrespeitá-las, ficarão sujeitos às sanções previstas em lei e normas externas.

5.2 A existência e o conteúdo deste Termo de Confidencialidade, bem como a execução das atividades dos empregados da EMPRESA a serviço do SESI-SP e do SENAI-SP não poderão ser reveladas a terceiros.

5.3 A seleção das informações confidenciais, a serem disponibilizadas para os empregados da EMPRESA será de exclusivo critério do SESI-SP e do SENAI-SP.

5.4 Fica expressamente entendido que ao revelar as informações confidenciais para a EMPRESA, o SESI-SP e o SENAI-SP não estarão concedendo qualquer tipo de licença, expressa ou implícita, nem transferindo direitos de qualquer espécie sobre tais informações.

5.5 As partes, no âmbito das relações de trabalho que mantêm com seus empregados e/ou prepostos, e nos limites e na proporção de suas responsabilidades, inclusive as de natureza tributária, responderão por todas as obrigações sociais, fiscais, parafiscais, trabalhistas, inclusive de previsão em normas coletivas das categorias, previdenciárias e sanitárias, que incidam ou venham a incidir sobre este Termo e; sobre os serviços eventualmente contratados, com terceiros, aí incluídas as relativas a acidentes de trabalho. Responderão, também, nas esferas civil e trabalhista pelos atos praticados por seus empregados e prepostos, quando da execução das atividades objeto deste Termo, suportando os ônus decorrentes de quaisquer danos, materiais e/ou morais, que os mesmos venham a causar aos bens e às pessoas.

CLÁUSULA SEXTA - DA DURAÇÃO

6.1 O acordo vigorará pelo período de 05 (cinco) anos contados da data de sua assinatura ou até o término do contrato que porventura venha a ser celebrado entre as partes, relacionado com o propósito deste acordo, podendo ser terminado, a qualquer tempo durante a sua vigência, por mútuo acordo entre as partes ou após notificação por escrito de uma parte à outra.

6.2 O término do acordo não desobriga as partes quanto às obrigações de confidencialidade aqui estipuladas anteriormente à efetiva data de seu encerramento, devendo a EMPRESA manter sigilo sobre as informações confidenciais recebidas por 5 (cinco) anos após sua recepção.

CLÁUSULA SÉTIMA - DAS PENALIDADES

7.1 A inobservância do dever de confidencialidade ora firmado e de qualquer das disposições deste instrumento é motivo relevante para o encerramento de toda e qualquer relação negocial existente entre as partes e a parte culpada será obrigada a ressarcir perdas e danos que venham a ocorrer à outra parte.

7.2 A EMPRESA será considerada infratora nos termos da legislação civil e criminal, na hipótese em que o sigilo da informação seja violado por qualquer pessoa a ela vinculada ou que tenha, por seu intermédio, obtido acesso às informações, exceto nos casos de caso fortuito e/ou força maior, se assim apurado.

CLÁUSULA OITAVA – DA ASSINATURA ELETRÔNICA

8.1. Quando for o caso, como alternativa à assinatura física, as Partes declaram e concordam que a assinatura deste Instrumento e todos os seus aditivos e afins poderá ser realizada eletronicamente.

8.2. As Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia deste Instrumento, de acordo com o art. 219 do Código Civil, em formato eletrônico e assinado pelas Partes por meio de certificados eletrônicos, nos termos do art. 10, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (“MP 2.200-2”), declarando, desde já, plena anuência com a aposição das assinaturas eletrônicas neste Contrato na plataforma a ser definida pelas Partes.

8.3. Adicionalmente, as Partes signatárias deste Instrumento expressamente anuem, autorizam, aceitam e reconhecem como válida qualquer forma de comprovação da autoria de suas respectivas assinaturas por meio de certificados eletrônicos, nos termos da MP 2.200-2, de 24/08/2001, sendo certo que quaisquer de tais certificados será suficiente para comprovar a veracidade, autenticidade, integridade, validade e eficácia deste Contrato e seus termos, bem como a respectiva vinculação das Partes às suas disposições, nos termos do artigos 441 e 784, III, do Código de Processo Civil.

CLÁUSULA NONA - DA REPRESENTAÇÃO DAS PARTES

As partes declaram neste ato, para todos os fins e efeitos de direito, que o(s) signatário(s) é(são) seu(s) legítimo(s) representante(s) na data de assinatura deste instrumento, estando cientes de que a falsidade na prestação desta informação, sem prejuízo de serem aplicadas as penalidades previstas neste instrumento, inclusive sua rescisão e apuração de perdas e danos, sujeitará todas as pessoas que para ela concorrem, às penalidades previstas na legislação criminal relativas à falsidade ideológica (art. 299 do Código Penal).

CLÁUSULA DÉCIMA - DO FORO

As Partes elegem o Foro da Comarca de São Paulo para dirimir qualquer litígio advindo deste contrato, com renúncia expressa de qualquer outro, ainda que privilegiado.

E, por estarem assim justas e contratadas, firmam o presente instrumento eletronicamente, considerando-se celebrado na data da última assinatura digital lançada pelas partes.

_____*(cidade)*_____*, data da última assinatura digital.*

SERVIÇO SOCIAL DA INDÚSTRIA – SESI
Departamento Regional de São Paulo

.....
(cargo do gestor)

SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL - SENAI
Departamento Regional de São Paulo

.....
(cargo do gestor)

CONTRATADA

_____

_____
Representante(s) Legal(is)
Nome(s):
Cargo(s):
RG(s):

Testemunhas:

_____
Nome:
RG n.º

_____
Nome:
RG n.º

CRONOGRAMA

PROCESSO DE SELEÇÃO COM DISPUTA ABERTA N.º 494/2026

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO, INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE DO TIPO *NEXT GENERATION FIREWALL* (NGFW) E RECURSOS DE SEGURANÇA, PARA ATENDIMENTO DAS NECESSIDADES DO SESI-SP E DO SENAI-SP

Eventos	Datas
Publicação	**10/11/2026**
Retirada do Chamamento Público	A partir de **10/11/2026** *site*: https://licitacoes-e2.bb.com.br/aop-inter-estatico/
Pedidos de Esclarecimentos	**De 10/11/2026 até 16/11/2026** *e-mail*: contservicos@sesisenaisp.org.br
Início da reunião pública de disputa de preços	**19/11/2026** as **14h30**