SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC/TOCANTINS
INSTRUMENTO CONVOCATÓRIO DE LICITAÇÃO – SENAC/TO/CC/11/2022

OBJETO: ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL DAS UNIDADES OPERATIVAS DO SENAC TOCANTINS

MODALIDADE: CONCORRÊNCIA – TIPO: MENOR PREÇO POR LOTE

PREÇO MÁXIMO ESTIMADO: R$ 443.802,62 (QUATROCENTOS E QUARENTA E TRES MIL OITOCENTOS E DOIS REAIS E SESSENTA E DOIS CENTAVOS)

DATA DE ABERTURA: 31 DE JANEIRO DE 2023

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – DEPARTAMENTO REGIONAL NO ESTADO DO TOCANTINS – SENAC/TO torna público aos interessados que realizará sessão pública às **09h do dia 31 de janeiro de 2023**, na sede da Administração Regional, localizada na Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas, estado do Tocantins, para recebimento dos 02 (dois) envelopes (Proposta Comercial e Documentos de Habilitação) referentes ao Processo de Licitação que tem como objeto **ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL DAS UNIDADES OPERATIVAS DO SENAC TOCANTINS,** de acordo com os elementos e especificações constantes deste EDITAL DE CONCORRÊNCIA N° 11/2022.

A concorrência será do tipo **MENOR PREÇO POR LOTE** será regida pelas condições deste Edital e pela Resolução SENAC n° 958/2012, de 18.09.12 publicada no D.O.U em 26.09.12, alterada pelas Resoluções nº 1.144/2020, de 21.08.2020, nº 1.187/2022, de 06.01.2022 e nº 1.205/2022, de 14.07.2022, todas do Conselho Nacional do SENAC. O processamento e julgamento serão realizados pela Comissão Permanente de Licitação designada através da Portaria nº 080/2020, do Conselho Regional do SENAC/TO.

O Instrumento Convocatório e seus Anexos estarão à disposição das empresas interessadas no site www.to.senac.br/licitacoes.

Possíveis **dúvidas, pedidos de esclarecimentos e/ou impugnações** sobre o presente Instrumento Convocatório e seus Anexos deverão ser encaminhados a Comissão Permanente de Licitação via e-mail no endereço cpl@to.senac.br, **até às 18h00min do dia 27 janeiro de 2023**.

Palmas Tocantins, 11 de janeiro de 2023.

LUNAH BRITO GOMES
Diretora Regional
SENAC/TO

EDITAL DE CONCORRÊNCIA Nº 11/2022

ÍNDICE

ITEM	Página
1. DO OBJETO	04
2. DO CRITÉRIO DE JULGAMENTO	04
3. DAS CONDIÇÕES DO PROCESSO LICITATÓRIO	05
4. DAS CONDIÇÕES DE CREDENCIAMENTO E PARTICIPAÇÃO	06
5. DA HABILITAÇÃO – ENVELOPE Nº 01	07
6. DA PROPOSTA COMERCIAL – ENVELOPE Nº 02	10
7. DOS PROCEDIMENTOS DE ENTREGA, ABERTURA E JULGAMENTO DOS ENVELOPES CONTENDO OS DOCUMENTOS DE HABILITAÇÃO E A PROPOSTA COMERCIAL	11
8. DOS RECURSOS	14
9. DO INSTRUMENTO DE CONTRATO OU DOCUMENTO EQUIVALENTE	15
10. DO CANCELAMENTO	16
11. DAS OBRIGAÇÕES DAS PARTES	17
12. DA FORMA E CONDIÇÕES DE PAGAMENTO	17
13. DA SUBCONTRATAÇÃO	18
14. DAS PENALIDADES	18
15. DAS DISPOSIÇÕES GERAIS	19
16. DOS ANEXOS AO INSTRUMENTO CONVOCATÓRIO	20
ANEXO I – TERMO DE REFERENCIA	22
ANEXO II – MODELO DE CARTA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL	65
ANEXO III – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (COM PODERES ESPECIAIS)	67
ANEXO IV – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (SEM PODERES ESPECIAIS)	68
ANEXO V – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO A RECURSO (REFERENTE À FASE DE HABILITAÇÃO E JULGAMENTO);	69
ANEXO VI – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO A RECURSO (REFERENTE À FASE DE	70

PROPOSTA);	
ANEXO VII – MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE IDADE	72
ANEXO VIII – MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS À HABILITAÇÃO;	73
ANEXO IX – MINUTA DO CONTRATO	74

O SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – DEPARTAMENTO REGIONAL NO ESTADO DO TOCANTINS – SENAC/TO, serviço social autônomo, pessoa jurídica de direito privado, entidade de formação profissional sem fins lucrativos, torna público aos interessados que realizará sessão pública às **09h do dia 31 de janeiro de 2023**, na sede da Administração Regional, localizada na Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas, estado do Tocantins, para recebimento dos 02 (dois) envelopes (Proposta Comercial de Preços e Documentos de Habilitação) referentes ao Procedimento de Licitação para **ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL DAS UNIDADES OPERATIVAS DO SENAC TOCANTINS** de acordo com os elementos e especificações constantes neste **EDITAL DE CONCORRÊNCIA N° 11/2022**. A concorrência, do tipo **MENOR PREÇO POR LOTE** será regida pelas condições deste Edital e pela Resolução SENAC n° 958/2012, de 18.09.12 publicada no D.O.U em 26.09.12, alterada pelas Resoluções nº 1.144/2020, de 21.08.2020 e nº 1.187/2022, de 06.01.2022, ambas do Conselho Nacional do SENAC. O processamento e julgamento serão realizados pela Comissão Permanente de Licitação designada através da Portaria nº 080/2022, do Conselho Regional do SENAC/TO.

1. DO OBJETO

1.1. A presente licitação, na modalidade **CONCORRÊNCIA**, do tipo **MENOR PREÇO POR LOTE**, tem por objeto a **atualização de solução de firewall das Unidades Operativas do Senac Tocantins**, em conformidade com o disposto no ANEXO I deste Edital e com o seguinte:

2. DO CRITÉRIO DE JULGAMENTO

2.1. O critério de julgamento da(s) proposta(s) vencedora(s) da presente licitação será o de MENOR PREÇO POR LOTE, **respeitados os valores unitários máximos aceitos por item** previstos no Anexo I, vinculado ao atendimento das exigências contidas neste Instrumento Convocatório e seus Anexos.

2.2. O preço máximo estimado da contratação é de **R$ 443.802,62 (quatrocentos e quarenta e três mil oitocentos e dois reais e sessenta e dois centavos),** observados os valores unitários previstos no ANEXO I.

2.3. Conforme previsto no art. 16 da Resolução Senac n. º 958/2012, será facultado à Comissão Permanente de licitação, inverter o procedimento, abrindo primeiro o envelope com as propostas, classificando os proponentes, e só então abrindo o envelope de habilitação do (s) licitante (s) classificado (s) em primeiro lugar.

3. DAS CONDIÇÕES DO PROCESSO LICITATÓRIO

3.1. Poderão habilitar-se no presente processo licitatório pessoas jurídicas que atuem em ramo de atividade compatível com o objeto da licitação, devendo apresentar os DOCUMENTOS DE HABILITAÇÃO necessários e a PROPOSTA COMERCIAL, de acordo com os itens 5 (cinco) e 6 (seis) deste Edital.

3.1.1 Os referidos documentos devem ser entregues à Comissão Permanente de Licitação até a data, hora e no local estabelecidos para tanto neste Instrumento Convocatório, em envelopes opacos, individualizados e devidamente fechados/lacrados (Envelope nº 01 – DOCUMENTOS DE HABILITAÇÃO e Envelope nº 02 – PROPOSTA COMERCIAL), para o fim a que se destinam.

3.2. Os envelopes deverão conter em sua parte externa e frontal o nome e endereço da licitante, com indicação de telefone, fac-símile e/ou e-mail para contato.

3.2.1 Modelo da parte frontal do envelope nº 01:

NOME DA LICITANTE:
CNPJ:
ENDEREÇO:
TELEFONE: E-MAIL: CEP:

AO
SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC/TO
COMISSÃO PERMANENTE DE LICITAÇÃO – SENAC/TO
Ref. CONCORRÊNCIA Nº 11/2022
OBJETO: **ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL DAS UNIDADES OPERATIVAS DO SENAC TOCANTINS.**
Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas - Tocantins.

ENVELOPE Nº 01 – DOCUMENTOS DE HABILITAÇÃO

MODELO

3.2.2. Modelo da parte frontal do envelope nº 02:

NOME DA LICITANTE:
CNPJ:

ENDEREÇO:

TELEFONE: E-MAIL: CEP:

AO

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC/TO

COMISSÃO PERMANENTE DE LICITAÇÃO – SENAC/TO

Ref. CONCORRÊNCIA Nº 11/2022

OBJETO: **ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL DAS UNIDADES OPERATIVAS DO SENAC TOCANTINS.**

Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas - Tocantins.

MODELO

ENVELOPE Nº 02 – PROPOSTA COMERCIAL

4. DAS CONDIÇÕES DE CREDENCIAMENTO E PARTICIPAÇÃO

4.1 No horário indicado no preâmbulo deste Edital, o representante legal da licitante apresentar-se-á ao Presidente da Comissão Permanente de Licitação para efetuar o seu credenciamento, munido da sua carteira de identidade, ou outro instrumento equivalente, e do documento que lhe dê poderes para manifestar-se durante a reunião de abertura dos envelopes **"DOCUMENTAÇÃO DE HABILITAÇÃO" e "PROPOSTA COMERCIAL"** relativa ao certame.

4.2. Considera-se representante legal qualquer pessoa habilitada pela **LICITANTE**, mediante **documento credencial.**

4.2.1 Entende-se por documento de credenciamento:

4.2.1.1 **Registro Comercial / Contrato Social / Estatuto**: Quando a pessoa credenciada for proprietária, sócia, dirigente ou assemelhada da empresa licitante, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura; ou

4.2.1.2 **Procuração, ou Documento Equivalente**: Aquele em que se concedem poderes para que a pessoa credenciada possa manifestar-se em qualquer fase deste certame em nome da licitante. Devendo estar acompanhada do original ou cópia do Contrato Social para confirmação da veracidade do outorgante.

4.2.1.3 Os documentos de credenciamento do representante serão entregues em separado e NÃO DEVEM ser colocados dentro de nenhum dos envelopes.

4.2.2 Os documentos mencionados no item 4.2.1, supra, deverão dar plenos poderes ao credenciado para declarar a intenção de interpor recursos, renunciar ao direito de interposição de recursos, enfim, para praticar em nome da licitante todos os atos pertinentes à reunião;

4.2.3 **Todos os documentos apresentados para efeito de credenciamento serão os originais ou fotocópias legíveis.** A responsabilidade pela capacidade da pessoa que assinar o instrumento de procuração ou documento equivalente será do representante que apresentar o aludido documento.

4.2.4 Cada licitante só poderá ser representada por uma única pessoa, não sendo admitido que uma mesma pessoa represente mais de uma empresa licitante, e nem que o representante de uma seja sócio de outra;
4.2.5 O representante legal que não se credenciar perante o Presidente da **CPL** ficará impedido de representar a licitante durante a reunião de abertura dos envelopes.

4.3 Em caso de não comparecimento do representante credenciado ao ato de recebimento e abertura dos envelopes, o documento de credenciamento juntamente com a fotocópia do documento de identidade deverá ser acondicionado no Envelope nº 01 – DOCUMENTOS DE HABILITAÇÃO.

4.4. Não poderão participar da presente licitação, nem contratar com o SENAC/TO:
4.4.1 Empresas sob o controle acionário de um mesmo grupo de pessoas físicas ou jurídicas;
4.4.2 Empresas em processo de falência ou em recuperação judicial ou extrajudicial;
4.4.3 Empresa temporariamente suspensa do direito de licitar ou contratar com o SENAC.

4.5. As licitantes deverão ter pleno conhecimento dos elementos constantes deste Edital, notadamente das condições gerais e particulares de seu objeto, não podendo invocar qualquer desconhecimento como elemento impeditivo da formulação da proposta e do integral cumprimento do contrato.

4.6 O prazo de encerramento de entrega dos envelopes se dará depois de rompido o primeiro envelope. Nenhum outro documento será recebido e nem serão permitidos adendos, acréscimos ou esclarecimentos à documentação e proposta, salvo a critério da Comissão Permanente de Licitação, para instruir eventuais impugnações interpostas na sessão.

4.7 A presença do representante não é obrigatória, porém os licitantes que não fizerem representar ficam logo desde já cientes que desta forma aceitam o que for decidido pela Comissão de licitação.

4.8 A simples participação da licitante na presente licitação dará consentimento na utilização dos dados necessários para atendimento das finalidades a que esse processo licitatório se propõe.

5. DOS DOCUMENTOS DE HABILITAÇÃO – ENVELOPE N°01

O Envelope nº 01 deverá conter, obrigatoriamente, os documentos a seguir relacionados, **originais ou fotocópias legíveis,** sob pena de inabilitação da licitante proponente.

5.1. HABILITAÇÃO JURÍDICA:

5.1.1 Registro Comercial no órgão competente, no caso de empresa individual.

5.1.2 Ato constitutivo (estatuto ou contrato social em vigor) devidamente registrado no órgão competente, em se tratando de sociedades comerciais; e no caso de sociedades por ações, além do ato constitutivo, os documentos de nomeação ou de eleição de seus atuais administradores, também devidamente registrados no órgão competente.
5.1.3 Cédula de Identidade (Válida em todo território nacional).

Observação: Documentos para habilitação jurídica conforme item 5.1, serão dispensados se já apresentados em fase anterior na licitação (Credenciamento)

5.2. REGULARIDADE FISCAL:

5.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ/MF;
5.2.2. Prova de regularidade para com a Fazenda Federal, Estadual e Municipal, do domicílio ou sede da licitante, na forma da lei, apresentando, para tal:
5.2.2.1. Certidão Conjunta Negativa de Débitos relativos a tributos federais e à dívida ativa da União, abrangendo inclusive as contribuições sociais previstas nas alíneas "a" e "d" do parágrafo único do art. 11 da Lei n.º 8.212, de 24 de julho de 1991;
5.2.2.2. Certidão Negativa de Débito de tributos estaduais;
5.2.2.3. Certidão Negativa de Débito de tributos municipais;
5.2.3. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (Certificado de Regularidade do FGTS – CRF);
5.2.4. Prova de regularidade perante a Justiça do Trabalho (Certidão Negativa de Débitos Trabalhistas – CNDT).

5.3. QUALIFICAÇÃO TÉCNICA:

5.3.1 Apresentação de, no mínimo, 01 (um) atestado de capacidade técnica (cuja data de emissão não será levada em consideração para efeitos de sua validade), impresso em papel timbrado da pessoa jurídica emitente, contendo a identificação do signatário e dados para eventual contato, emitido por pessoa de direito público e/ou privado **(sujeito à promoção de diligência)** para as quais a licitante tenha prestado ou esteja prestando serviços similares aos dos objetos deste processo licitatório (visando comprovar sua aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação).

Observação: o teor do documento em questão deve possibilitar à Comissão Permanente de Licitação a análise, interpretação e conclusão, de forma clara e sem maiores dificuldades, acerca do seu objeto, visando apurar se atende ou não às condições a que se destina ou propõe.

5.4. DECLARAÇÕES:

5.4.1 **Declaração**, para fins de cumprimento do disposto no inciso XXXIII do Art. 7º da Constituição Federal, **de que não emprega menores**, conforme modelo constante do ANEXO VII deste EDITAL.
5.4.2 **Declaração de inexistência de fatos impeditivos à habilitação** e ciência da obrigatoriedade de comunicação de fatos supervenientes, conforme modelo constante do ANEXO VIII deste EDITAL.

5.5. OBSERVAÇÕES QUANTO À DOCUMENTAÇÃO EXIGIDA NA FASE DE HABILITAÇÃO:

5.5.1 Toda a documentação apresentada deverá estar em plena vigência. Documentos omissos quanto ao prazo de validade (à exceção daqueles com prazos de validade estabelecidos por este Edital) serão aceitos apenas se tiverem sido emitidos nos 90 (noventa) dias corridos anteriores à sua apresentação à Comissão Permanente de Licitação.
5.5.2 Todas as certidões obtidas via Internet somente serão aceitas como documentação hábil para o fim a que se destinam após a verificação pela Comissão Permanente de Licitação, se esta entender necessário, da sua regularidade, validade e autenticidade, por meio de diligências junto aos respectivos órgãos oficiais expedidores.
5.5.3 Para fins de habilitação, a verificação pelo SENAC nos sítios oficiais de órgãos e entidades emissores de certidões também constitui meio legal de prova;
5.5.4 Para a licitante ter direito à participação ativa na sessão pública de recebimento dos Envelopes de números 01 e 02 (contendo, respectivamente, os Documentos de Habilitação e a Proposta Comercial), faz-se necessária a identificação do seu preposto perante a Comissão Permanente de Licitação, mediante a apresentação de procuração por instrumento público ou particular (neste caso, devidamente assinada por pessoa com poderes para tal) ou da autorização para representá-la (AUTORIZAÇÃO DE REPRESENTAÇÃO – ANEXOS III e IV deste Edital), bem como do respectivo documento de identificação e do Ato Constitutivo (estatuto ou contrato social) da licitante.

5.5.4.1 No caso de o representante legal participar pessoalmente da sessão pública, a sua identificação será feita mediante apresentação do Ato Constitutivo (estatuto ou contrato social) da licitante e de documento pessoal de identificação deste.

5.5.4.2 **Os mesmos documentos serão exigidos para a interposição de recursos**.

5.5.5 Sugere-se, ainda, com o propósito de agilizar o processo licitatório, a utilização simultânea e opcional da DECLARAÇÃO DE RENÚNCIA QUANTO A RECURSO, conforme modelos constantes dos ANEXOS V E VI deste Edital. Observação: Recomenda-se que tais documentos sejam apresentados separadamente dos envelopes contendo os DOCUMENTOS DE HABILITAÇÃO e a PROPOSTA COMERCIAL.
5.5.6 Os documentos que exigem assinatura somente serão aceitos se assinados pelo representante legal da empresa, de acordo com o disposto no respectivo ato constitutivo, procuração específica ou

Autorização de Representação com Poderes Especiais, conforme o modelo constante do ANEXO V deste EDITAL.

6. DA PROPOSTA COMERCIAL – ENVELOPE Nº 02

6.1. A CARTA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL (conforme modelo constante do ANEXO II deste Edital) deverá ser apresentada em papel timbrado da empresa licitante, em 01 (uma) via, digitada ou datilografada, em linguagem clara, sem emendas ou rasuras, datada e devidamente assinada pelo representante legal da empresa, e deverá conter as seguintes informações:

6.1.1. Razão Social ou denominação da licitante e número de sua inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ/MF;

6.1.2. Objeto da Licitação: conforme descrito no Item 1 deste Instrumento Convocatório;

6.1.3. Preço cotado: em moeda nacional, em algarismos e por extenso, aí já incluídos tributos, fretes, seguros e outras despesas, encargos e/ou ônus, seja a que título for, necessários ao cumprimento do objeto da licitação, de acordo com as condições e/ou especificações constantes do ANEXO I deste Edital e observado o disposto no subitem 6.2 abaixo;

6.1.4. Prazo de validade da Proposta Comercial: **não poderá ser inferior a 90 (noventa) dias**, contados a partir da data prevista para a abertura da licitação e entrega/recebimento dos Envelopes nº 01 (Documentos de Habilitação) e nº 02 (Proposta Comercial);

6.1.5. Prazo de entrega: de no máximo **45 (quarenta e cinco) dias consecutivos**, contados da data de assinatura do contrato e autorização do fornecimento;

6.1.6. Forma e condições de pagamento: deverão estar em consonância com o estabelecido no Item 12 deste Instrumento Convocatório;

6.1.7. Identificação do representante legal da empresa: responsável por assinar o instrumento de contrato ou documento equivalente, no caso de a licitante ser declarada vencedora do certame.

6.2. O(s) licitante(s) deverá (ão) incluir, junto com a respectiva PROPOSTA COMERCIAL, informações adicionais, **catálogos, manuais, folders, encartes, prospectos, enfim, quaisquer outros elementos elucidativos, referentes aos equipamentos cotados**, (material impresso e/ou arquivo digital e/ou indicação da URL do fabricante que permita comprovar as especificações técnicas dos equipamentos ofertados), com o fim de possibilitar à área técnica do SENAC/TO fazer a análise prévia e validação de tais equipamentos, nos termos e condições/especificações constantes deste Edital e seus Anexos;

6.3. O valor ofertado será representado pelo menor preço por LOTE, respeitados os valores máximos aceitos por item, previstos no Anexo I deste Edital, sob pena de **desclassificação** da Proposta;

6.4. O valor ofertado na proposta estará limitado à duas casas decimais após a virgula, entenda-se, se o licitante ofertar proposta com mais de duas casas após a virgula, da terceira casa em diante, serão desprezadas para critério de julgamento;

6.5. O ato de apresentação da Proposta Comercial pela empresa licitante será considerado como evidência de que examinou, em sua plenitude, todos os dados e/ou especificações do presente Instrumento Convocatório e seus Anexos, e que não tem nenhuma dúvida com relação aos seus termos, implicando, por conseguinte, a aceitação tácita de todas as cláusulas e termos deste Edital;

6.6. Após a fase de habilitação não cabe desistência da proposta, salvo por motivo justo decorrente de fato superveniente e aceito pela Comissão Permanente de Licitação;

7. DOS PROCEDIMENTOS DE ENTREGA, ABERTURA E JULGAMENTO DOS ENVELOPES CONTENDO OS DOCUMENTOS DE HABILITAÇÃO E A PROPOSTA COMERCIAL

7.1. DA ENTREGA DOS 02 (DOIS) ENVELOPES CONTENDO OS DOCUMENTOS DE HABILITAÇÃO E A PROPOSTA COMERCIAL:

7.1.1. **No dia 31 de janeiro de 2023, às 09h**, na sede da Administração Regional, localizada na Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas - TO, a Comissão Permanente de Licitação receberá os 02 (dois) Envelopes contendo os Documentos de Habilitação e a Proposta Comercial, devidamente fechados e lacrados.

7.1.2. Não serão aceitos Envelopes (Documentos de Habilitação e Proposta Comercial) após o dia e horário estabelecidos para tal no presente Instrumento Convocatório.

7.1.3. Depois de encerrado o prazo de recebimento dos Envelopes, nenhum outro documento será aceito pela Comissão Permanente de Licitação, bem como, a partir daí, não mais serão permitidos adendos, acréscimos ou substituições, sobre os documentos regularmente recebidos.

7.2. DA ABERTURA DO ENVELOPE Nº 01 (DOCUMENTOS DE HABILITAÇÃO):

7.2.1. Encerrado o prazo para recebimento dos envelopes, será efetuada, imediatamente, a abertura do Envelope nº 01 (Documentos de Habilitação). As licitantes ou pessoas autorizadas por estas que desejem participar ativamente da referida sessão pública devem observar o disposto no subitem 5.6.4 e os demais termos previstos neste Instrumento Convocatório.

7.2.2. Os Documentos de Habilitação serão rubricados pelos membros da Comissão Permanente de Licitação e pelos representantes das empresas licitantes presentes à sessão, que assim desejarem.

7.2.3. Na sequência, os membros da Comissão Permanente de Licitação e os representantes das empresas licitantes presentes à sessão procederão à rubrica dos Envelopes nº 02 (Proposta Comercial). Os envelopes serão mantidos pela Comissão Permanente de Licitação até a data de sua abertura, em hora e local a serem por ela definidos.

7.2.4. Ao final da sessão pública será lavrada ata, da qual constará o(s) nome(s) da(s) licitante(s) e seu(s) representante(s) legal(is), bem como todas as ocorrências que interessem aos participantes e ao SENAC/TO, devendo esta ser lida, posta em discussão, aprovada e assinada pelos membros da

Comissão Permanente de Licitação e pelos representante(s) legal(is) da(s) licitante(s) presente(s) à sessão.

7.3. DA ANÁLISE E JULGAMENTO DOS DOCUMENTOS DE HABILITAÇÃO:

7.3.1. Se durante a sessão pública não for possível avançar com o procedimento, a critério da Comissão Permanente de Licitação, esta realizará o julgamento dos Documentos de Habilitação das licitantes, comunicando o resultado aos interessados através do site www.to.senac.br.

7.3.2. Após o transcurso dos prazos relativos à fase recursal, exceto no caso de renúncia expressa à faculdade de interpor recursos por parte de todas as licitantes, a Comissão Permanente de Licitação comunicará às licitantes habilitadas, com antecedência mínima de 02 (dois) dias úteis, a data, hora e local da sessão de abertura do(s) Envelope(s) nº 02 – Proposta Comercial, através do site www.to.senac.br e/ou via fac-símile e/ou e-mail.

7.3.3. O Envelope nº 02 (Proposta Comercial) de empresa licitante eventualmente não habilitada para a fase seguinte do certame, desde que não tenha havido recurso ou este tenha sido improvido, será mantido fechado e lacrado pela Comissão Permanente de Licitação e eficará disponível para devolução, mediante protocolo, quando esta desejar apanhá-lo junto à Comissão Permanente de Licitação.

7.4. DA ABERTURA DO ENVELOPE Nº 02 (PROPOSTA COMERCIAL):

7.4.1. A Comissão Permanente de Licitação, na data, hora e local estabelecidos para tal, procederá à abertura do(s) Envelope(s) nº 02 – Proposta(s) Comercial(is) e fará a leitura dos valores de seus itens, sendo, então, a(s) proposta(s) rubricada(s), folha a folha, pelos membros da Comissão Permanente de Licitação e representante(s) da(s) empresa(s) licitante(s) presente(s) à sessão.

7.4.2. Da referida sessão será lavrada ata, da qual constará o(s) nome(s) do(s) representante(s) da(s) empresa(s) licitante(s) presente(s), o(s) preço(s) proposto(s) e todas as ocorrências julgadas de interesse, devendo a ata ser lida, posta em discussão, aprovada e, ao final, assinada pelos membros da Comissão Permanente de Licitação e representante(s) da(s) empresa(s) licitante(s) presente(s) à sessão.

7.4.3. Ultrapassada a fase de habilitação e uma vez aberta(s) a(s) Proposta(s) Comercial(is), não mais caberá desclassificar a(s) licitante(s) remanescente(s) por motivos relacionados à fase anterior (de habilitação), salvo em razão de fatos supervenientes ou só conhecidos após o seu julgamento, que possam desabonar ou, até mesmo, inviabilizar o cumprimento da obrigação decorrente do objeto deste processo licitatório pela empresa licitante declarada vencedora do certame.

7.5. DA ANÁLISE E JULGAMENTO DAS PROPOSTAS:

7.5.1. Após a abertura do(s) Envelope(s) n° 02 (Proposta Comercial), na mesma sessão ou em momento posterior, a critério da Comissão Permanente de Licitação, considerados os termos deste Instrumento

Convocatório e seus Anexos, a(s) Proposta(s) Comercial(is) será(ão) analisada(s) quanto a eventuais erros aritméticos, os quais, uma vez constatados, serão corrigidos pela Comissão da seguinte forma:

7.5.1.1. Em caso de divergência entres o(s) preço(s) unitário(s) e o total, prevalecerá(ão) o(s) preço(s) unitário(s), recalculando-se, consequentemente, o preço total.

7.5.1.2. Ocorrendo divergência entre os valores numéricos e por extenso, prevalecerá este último (extenso).

7.5.2. Em até 05 (cinco) dias úteis após a abertura da(s) Proposta(s) Comercial(is), a Comissão Permanente de Licitação definirá, através de julgamento devidamente fundamentado, a empresa licitante detentora da melhor Proposta e, consequentemente, aquela a ser declarada vencedora do certame, a qual ficará vinculada às exigências e/ou condições constantes deste Instrumento Convocatório e seus anexos, comunicando o resultado a todos os interessados através do site www.to.senac.br.

7.5.3. Ocorrendo empate entre 02 (duas) ou mais propostas, o desempate dar-se-á através de sorteio realizado pela Comissão Permanente de Licitação, em sessão pública, cujo local, data e horário serão previamente definidos e formalmente comunicados aos interessados pela Comissão.

7.5.4. No julgamento das propostas e da habilitação, a Comissão Permanente de Licitação poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos exigidos neste Edital, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação e habilitação;

7.5.5. Serão desclassificadas as Propostas Comerciais que:

7.5.5.1 Estejam em desacordo com o presente instrumento convocatório, em especial aquelas que:

a) Impuserem condições não previstas neste edital;

b) Contenham prazo de validade inferior a 90 (noventa) dias;

c) Não observem os valores máximos aceitos obtidos através de propostas de preços realizadas no mercado;

7.5.6. A Comissão Permanente de Licitação e/ou a autoridade competente para tal poderá(ão) pedir esclarecimentos e promover diligências, em qualquer fase da licitação e sempre que assim julgar necessário, inclusive fixando prazos para atendimento de eventuais questionamentos por quem de direito, objetivando elucidar eventuais dúvidas ou complementar a instrução do processo, vedada, no entanto, a inclusão posterior de documentos e/ou informações que deveriam constar, originalmente, da(s) Proposta(s) Comercial (is). Também poderá(ão) realizar visita técnica às dependências e/ou instalações da empresa licitante, a fim de verificar se esta dispõe de infraestrutura que a permita, uma vez declarada vencedora do certame, atender plenamente ao objeto desta licitação, na forma e condições previstas no presente instrumento convocatório e seus anexos.

7.5.7. A Comissão Permanente de Licitação, antes ou após a adjudicação o objeto ao vencedor do certame, poderá solicitar amostras dos equipamentos, quando for o caso, para avaliação de questões técnicas, caso as informações adicionais, catálogos e quaisquer outros elementos elucidativos, referentes aos produtos cotados sejam incompletos;

7.5.7.1. As amostras serão apresentadas na data e local designados pela Comissão Permanente de Licitação. A não apresentação das amostras solicitadas, por parte da(s) empresa(s) classificada(s) em primeiro lugar, dentro do prazo estabelecido, ocasionará a desclassificação da(s) licitante(s), sendo convocados, por ordem de classificação, os demais participantes do processo licitatório.

7.5.8. Transcorridos os prazos relativos à fase recursal ou se tiver havido renúncia expressa ao direito de interpor recursos por parte de todas as licitantes, a Comissão Permanente de Licitação remeterá o processo licitatório à autoridade competente para homologação do resultado do julgamento do certame, bem como para adjudicação do seu objeto à(s) empresa(s) licitante(s) declarada(s) vencedora(s) o que, no entanto, não impedirá que a autoridade competente, por meio de despacho fundamentado e no exclusivo interesse do SENAC/TO, presentes os requisitos legais para tanto, revogue, anule ou cancele a licitação, sem que de tal ato caiba qualquer reivindicação de pretenso direito, por quem quer que seja, a qualquer título.

7.5.9. Se todas as licitantes forem inabilitadas (fase de habilitação) ou todas as propostas forem desclassificadas (fase de julgamento das propostas), a Comissão de Licitação poderá conceder às licitantes o prazo de 08 (oito) dias úteis para a apresentação de nova documentação ou de outras propostas, escoimadas dos vícios que ensejaram a inabilitação ou a desclassificação.

7.5.10 Poderá a Comissão Permanente de Licitações deliberar pela inversão do procedimento licitatório, abrindo primeiramente as propostas de preço, classificando os proponentes, e só então abrir o envelope de habilitação da(s) licitante(s) classificada(s) em 1º lugar;

7.5.11 Se a(s) licitante(s) classificada(s) em 1º lugar forem inabilitadas, após julgados eventuais recursos interpostos, proceder-se-á a abertura dos envelopes de habilitação dos licitantes remanescentes, na ordem de classificação desses, para que o seguinte classificado que preencha as condições de habilitação seja declarado vencedor, em iguais condições, inclusive quanto ao preço, do licitante classificado em 1º lugar;

7.5.12 Os Envelopes das empresas licitantes eventualmente não habilitada, desde que não tenha havido recurso ou este tenha sido improvido, será mantido fechado e lacrado pela Comissão Permanente de Licitação e devolvido à licitante diretamente, mediante protocolo, logo após a homologação de certame. Após esse período, os envelopes e conteúdo do mesmo serão inutilizados.

8. DOS RECURSOS

8.1. Salvo se tiver havido renúncia expressa por parte de todas as licitantes, caberá recurso à autoridade competente, o qual deverá ser interposto perante a Comissão Permanente de Licitação, por escrito e devidamente fundamentado, no prazo de 05 (cinco) dias úteis, contados da comunicação da decisão acerca:

a) Da habilitação ou inabilitação da licitante;

b) Do julgamento da(s) Proposta(s).

8.1.1. O(s) recurso(s) deverá(ão) ser interposto(s) perante a Comissão Permanente de Licitação, mediante protocolo, do qual deverá constar, obrigatoriamente, a data e a hora de sua interposição,

observando-se, para tanto, o horário das 08h30min às 12h e das 14h às 18h, dos dias úteis de expediente do SENAC/TO.
8.1.2. O(s) recurso(s) referente(s) à fase de Habilitação terá(ão) efeito suspensivo; já o(s) recurso(s) referentes ao julgamento da(s) Proposta(s) terá(ão) efeito suspensivo por lote e/ou item.

8.2. Interposto(s) o(s) recurso(s), abrir-se-á vista dele(s) às demais licitantes, pelo prazo comum de 05 (cinco) dias úteis, contados da data da comunicação da interposição, para eventual contrarrazões por quem de direito, as quais devem ser apresentadas dentro desse prazo, sobrestando-se a remessa do processo licitatório à autoridade competente para o julgamento.

8.3. Contra-arrazoado(s) ou não o(s) recurso(s), a Comissão Permanente de Licitação os apreciará, podendo, se necessário, realizar instrução complementar, e decidirá, motivadamente, pela manutenção ou reforma do ato recorrido, no prazo de até 05 (cinco) dias úteis contados do encerramento do prazo para apresentação de contrarrazões, encaminhando, em seguida, o respectivo processo à autoridade competente para os devidos fins.

8.4. O(s) recurso(s) eventualmente interposto(s) será(ão) julgado(s), em única e última instância, pela autoridade competente ou por quem esta delegar competência, no prazo de até 10 (dez) dias úteis, e o resultado será comunicado ao(s) interessado(s) através do site www.to.senac.br e por e-mail.

8.5. Eventual(is) recurso(s) interposto(s) fora do prazo definido para tal não será(ão) conhecido(s).

8.6. É facultado a qualquer licitante formular impugnações ou protestos, por escrito, devidamente registrados na ata dos respectivos trabalhos, em relação a qualquer das demais licitantes ou ao transcurso da licitação.

9. DO INSTRUMENTO DE CONTRATO OU DOCUMENTO EQUIVALENTE

9.1. Uma vez homologado o processo licitatório e feita a adjudicação pela autoridade competente (ou por quem esta delegar competência), a Comissão Permanente de Licitação convocará, via e-mail, correio ou fac-símile, em até 05 (cinco) dias úteis, a(s) empresa(s) licitante(s) declarada(s) vencedora(s) do certame para, em dia, hora e local designados, assinar(em) o respectivo contrato, assumindo assim, entre outras responsabilidades previstas no referido documento ou neste instrumento convocatório e seus anexos, o seu compromisso de execução do objeto deste processo licitatório.

9.2. Caso a(s) licitante(s) classificada(s) em primeiro lugar não atenda(m) à convocação para a assinatura do contrato ou, injustificadamente, recuse(m)-se a assiná-lo, a critério da Comissão Permanente de Licitação, ela decairá de todos os direitos ali constantes e poderá ser penalizada com

a suspensão do direito de licitar ou contratar com o SENAC/TO por até 2 (dois) anos, sem prejuízo de outras penalidades e/ou cominações legais eventualmente aplicáveis à espécie.

9.3. No caso do disposto no subitem anterior, poderá o SENAC/TO, desde logo, convocar a licitante classificada em segundo lugar (quando possível) para assinar o contrato, também em até 05 (cinco) dias úteis, e assim sucessivamente.

9.4. Decorrido o prazo de validade das propostas sem a convocação das licitantes classificadas para a assinatura do contrato, ficam estas liberadas dos compromissos assumidos por conta deste processo licitatório.

9.5. É facultado ao SENAC/TO, quando a licitante convocada se recusar a assinar o instrumento de contrato ou documento equivalente, convocar a(s) licitante(s) remanescente(s), na ordem de classificação (se possível), para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira classificada, ou revogar a licitação.

9.6. O disposto no subitem 9.2. não se aplica àquelas licitantes convocadas nos termos do subitem 9.5 que, eventualmente, não aceitarem a contratação nas mesmas condições propostas pela licitante classificada em primeiro lugar.

9.7. Os preços apresentados para presente licitação serão fixos e irreajustáveis.

10. DO CANCELAMENTO

10.1. O licitante perderá direito sobre a contratação quando:
10.1.1. Descumprir as condições assumidas em contrato;
10.1.2. Não assinar o contrato ou instrumento equivalente, no prazo estabelecido pelo SENAC/TO, sem justificativa aceitável para tal;
10.1.3. Quando, justificadamente, não for mais do interesse do SENAC/TO.

10.2. O eventual cancelamento do contrato pelo SENAC/TO nas hipóteses previstas, assegurado à licitante o direito ao contraditório e à ampla defesa, será formalizado por despacho fundamentado da autoridade competente para tal.

10.3. A licitante poderá solicitar o cancelamento do contrato na ocorrência de fato superveniente que venha a comprometer a perfeita execução contratual, decorrente de caso fortuito ou motivo de força maior, devidamente comprovado e que venha ser aceito pelo SENAC/TO.

10.4. A eventual solicitação de cancelamento do contrato que não atenda aos requisitos do subitem anterior será considerada como descumprimento total das obrigações, ficando a licitante sujeita às penalidades cabíveis.

11. DAS OBRIGAÇÕES DAS PARTES

11.1. Sem prejuízo das obrigações inerentes à perfeita execução do objeto da Licitação e demais disposições deste Instrumento, constituem obrigações das partes aquelas elencadas na Minuta do contrato e ANEXO I deste Edital.

12. DA FORMA E CONDIÇÕES DE PAGAMENTO

12.1. O prazo estipulado para o pagamento do valor devido por conta do objeto deste processo licitatório é de 20 (vinte) dias corridos, contados a partir da data de entrega dos equipamentos e apresentação do(s) competente(s) Documento(s) Fiscal(is), após atesto do recebimento pelo setor técnico do SENAC/TO.

12.2. O pagamento será efetuado por meio de depósito bancário, em banco, agência e conta corrente indicados pela licitante eventualmente contratada, observando-se a situação tributária desta, informada em papel com timbre da licitante no momento da contratação, obedecidas as disposições legais vigentes.

12.3. Nenhum pagamento será efetuado à licitante vencedora enquanto estiver pendente de liquidação qualquer obrigação, em especial, quando os documentos comprobatórios de situação regular em relação ao INSS, ao FGTS, à Fazenda Nacional, Estadual e Municipal, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, de modo que o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

12.4. Em caso de eventual divergência entre os documentos de cobrança e os preços contratados, a licitante terá prazo de até 03 (três) dias úteis para proceder à regularização ou substituição dos referidos documentos.

12.5. Em caso de eventual entrega parcial, não será efetuado o pagamento enquanto não ocorrer o adimplemento total da obrigação.

13. DA SUBCONTRATAÇÃO

13.1. A licitante assume integral responsabilidade pelos danos que, eventualmente, vier a causar ao SENAC/TO, e, salvo disposições em contrário, não poderá ceder, transferir ou subcontratar, no todo ou em parte, o objeto deste processo licitatório, a quem quer que seja, sem a prévia e expressa anuência destes.

13.2. A licitante será a única e exclusiva responsável pela eventual contratação de empregados e/ou terceiros prestadores de serviços em razão do objeto deste processo licitatório, e, consequentemente, dos ônus daí decorrentes, seja a que título for (salários e/ou remunerações, encargos sociais, trabalhistas, previdenciários, fiscais e/ou comerciais), eximindo, totalmente, o SENAC/TO de quaisquer possíveis atribuições de responsabilidade nesse particular, seja a que título for (de cunho solidário e/ou subsidiário).

14. DAS PENALIDADES

14.1. A recusa injustificada em assinar o instrumento de contrato e/ou documento equivalente, no prazo estabelecido para tal, caracterizará o descumprimento total da obrigação assumida e poderá acarretar à licitante as seguintes penalidades:
14.1.1. Perda do direito à contratação.
14.1.2. Suspensão do direito de licitar ou contratar com o SENAC por até 02 (dois) anos.

14.2. O inadimplemento total ou parcial das obrigações contratuais assumidas dará ao SENAC/TO o direito de rescindir unilateralmente o contrato, sem prejuízo de outras penalidades previstas neste Instrumento Convocatório ou no contrato ou documento equivalente, em especial:
14.2.1. Advertência por escrito.
14.2.2. Multa de 0,33% (trinta e três centésimos por cento) por dia de atraso na entrega dos equipamentos, calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, para atrasos de até 10 (dez) dias corridos em relação à data prevista para o cumprimento da obrigação em sua totalidade.
14.2.3. Multa de 10% (dez por cento), não cumulativa com a multa prevista no subitem 14.2.2 acima, calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, para atrasos acima de 10 (dez) dias corridos em relação à data prevista para o cumprimento da obrigação em sua totalidade, ou por seu não cumprimento.
14.2.4. Multa de 2% (dois por cento), calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, por qualquer outro incidente que configure o descumprimento das obrigações contratadas, com exceção daqueles especificados nos subitens 14.2.2 e 14.2.3 acima.
14.2.5. Suspensão do direito de licitar ou contratar com o SENAC por até 02 (dois) anos.

14.3. As penalidades de cunho pecuniário eventualmente impostas à licitante eventualmente contratada por conta do objeto deste terão seus valores descontados dos possíveis créditos que esta disponha junto ao SENAC/TO, decorrentes de parcelas vencidas e ainda não pagas ou parcelas vincendas, ou ainda, recolhidos diretamente junto à área financeira deste, no prazo de até 15 (quinze) dias corridos, contados da data da sua comunicação, ou, ainda, cobrados judicialmente, quando assim se fizer necessário ou se justificar. Neste caso, as despesas processuais e os honorários advocatícios serão custeados pela licitante eventualmente contratada.

14.4. É facultado à entidade licitadora exigir, ainda, da(s) empresa(s) licitante(s) declarada(s) vencedora(s) do certame que não cumprir(em) as obrigações assumidas por conta deste processo licitatório indenização por eventuais perdas e danos, nos termos do artigo 389 do Código Civil, sem prejuízo de outras penalidades contratuais e/ou legais aplicáveis à espécie, no que couber, em especial aquelas constantes da Lei nº 8.078, de 11.10.90 (Código de Defesa do Consumidor).

15. DAS DISPOSIÇÕES GERAIS

15.1. As licitantes deverão examinar, cuidadosamente, todos os termos e condições deste Edital de Licitação, a fim de se certificarem do seu inteiro teor, objetivando o correto e pleno cumprimento de seus termos.

15.2. As licitantes assumem, desde logo, todos os custos de preparação e apresentação das suas propostas, eximindo o SENAC/TO de qualquer atribuição de responsabilidade nesse particular, seja a que título for.

15.3. As licitantes são responsáveis diretas pela fidedignidade e/ou legitimidade das informações e documentos por elas apresentados juntamente com suas propostas.

15.4. O SENAC/TO se reserva o direito de adiar, revogar, anular, tornar sem efeito ou suspender, no todo ou em parte, temporária ou definitivamente, a presente licitação, inclusive de proceder a seu cancelamento (de forma justificada e desde que antes da assinatura do respectivo instrumento de contrato ou documento equivalente), sem que de tais atos caibam quaisquer possíveis direitos às licitantes, seja a que título for.

15.4.1. No caso de suspensão temporária da licitação, ficará a proponente liberada do compromisso de contratar com o SENAC/TO, sem qualquer penalidade, após o prazo de validade da sua proposta.

15.5. A empresa licitante, uma vez contratada, obrigar-se-á, com integral obediência às disposições deste Edital e seus Anexos, a responder pelo cumprimento de sua Proposta, em todos os seus termos.

15.6. A participação da empresa licitante neste processo licitatório implica o conhecimento e a aceitação de todos os termos deste Edital e seus Anexos.

15.7. Todos os documentos relacionados com a presente licitação são complementares entre si e assim devem ser considerados, mesmo quando um detalhe for mencionado em um documento e, eventualmente, omitido em outro.

15.8. O edital de licitação e todos os documentos que compõem o processo licitatório encontrar-se-ão disponíveis para consulta até a sua finalização no horário das 08h00min às 12h00min e das 14h00min às 18h00min, dos dias úteis de expediente do SENAC/TO, na Coordenação de Compras e Licitações, localizada na Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas - TO.

15.9. Os prazos estabelecidos no presente Edital e seus anexos só se iniciam e vencem em dias de funcionamento/expediente do SENAC/TO.

15.10. Qualquer conduta caracterizada como prejudicial ao bom andamento do certame licitatório poderá ser considerada como incursa no preceito do artigo 335 do Código Penal Brasileiro, ficando a licitante que der causa a tanto sujeita às penalidades legais cabíveis.

15.11. No julgamento das propostas e da habilitação, a Comissão Permanente de Licitação poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos exigidos neste Edital, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação e habilitação.

15.12. Os casos não previstos neste Edital serão decididos pela Comissão Permanente de Licitação com base nas disposições legais aplicáveis à espécie, no que couber.

15.13. A proposta, após sua abertura, vincula o licitante aos termos do presente Edital e da Resolução Senac n. º 958/2012.

16. DOS ANEXOS AO INSTRUMENTO CONVOCATÓRIO

16.1. Os anexos ao presente Edital são os seguintes:
16.1.1. ANEXO I – TERMO DE REFERENCIA;
16.1.2. ANEXO II – MODELO DE CARTA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL;
16.1.3. ANEXO III – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (com poderes especiais);
16.1.4. ANEXO IV – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (sem poderes especiais);

16.1.5. ANEXO V – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO A RECURSO (referente à fase de Habilitação e Julgamento);
16.1.6. ANEXO VI – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO A RECURSO (referente à fase de proposta);
16.1.7. ANEXO VII – MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE IDADE
16.1.8. ANEXO VIII – MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS À HABILITAÇÃO;
16.1.9. ANEXO IX – MINUTA DO CONTRATO
16.2. O Instrumento Convocatório e seus Anexos estarão à disposição das empresas interessadas no site www.to.senac.br/licitacoes.html e na Sede do Departamento Regional do SENAC/TO, Coordenação de Compras e Licitações, Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas - TO. Outras informações, esclarecimentos ou impugnações ao edital poderão ser encaminhadas para o e-mail cpl@to.senac.br, até às 18h do dia 27 de janeiro de 2023.

Palmas Tocantins, 11 de janeiro de 2023.

LUNAH BRITO GOMES
Diretora Regional
SENAC/TO

CONCORRÊNCIA PUBLICA N.º 11.2022 SENAC DR/TO

ANEXO I - TERMO DE REFERÊNCIA

1. OBJETO

O objeto da presente licitação é a escolha da proposta mais vantajosa representada pelo menor preço por lote para **CONTRATAÇÃO DE ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL SONICWALL**, **podendo ser ofertado soluções de outros fabricantes que atendam as condições e especificações constantes deste Termo de Referência**, visando atender as necessidades do SENAC/TO, conforme condições, quantidades e exigências estabelecidas neste termo de referência e seus anexos;

2. JUSTIFICATIVA DA CONTRATAÇÃO

Uma Solução de Firewall para uma rede de computadores consiste em filtros que controlam as conexões e comunicações que trafegam de uma rede para outra, cujos filtros possuem a ação de permitir ou negar o acesso entre redes. Com o bloqueio de tráfegos indesejados ocorre o impedimento de ataques e tráfego malicioso nas redes protegidas pela solução de firewall.

Entre as várias ações de segurança capaz de implementação em um firewall pode-se citar: ajuda a impedir que a rede, servidores e ativos sejam acessados sem autorização; evita que informações sejam capturadas; bloqueio de programas indesejados na rede como compartilhamento de dados e de mensagens instantâneas; fechamento de portas não utilizadas a fim de evitar abusos na utilização da Internet; permite auditoria nos acessos a recursos da rede; permite a limitação de banda por serviços e monitoramentos dos links de dados que passam por ele.

Por meio da **Concorrência Pública nº 03/2019**, ocorrida no ano de 2019, originou-se a aquisição da Solução de Firewall para Segurança de Rede do SENAC/TO. A aquisição e implementação da solução de segurança para a Rede do SENAC/TO teve como objetivos:

- Evitar uso indevido da rede e acessos não autorizados;
- Implantar o uso de VPN (Rede virtual privada) nas diversas unidades operativas do SENAC/TO;
- Disponibilizar com segurança vários serviços para acesso por meio da internet, como: SIG, correio eletrônico, Gestão de Folha de Pagamento, Gestão do Sistema de Ponto, Gestão Financeira, Gestão de RH, dentre outros;
- Atender o Plano Diretor para a área de TI (PDTI), com a adequação da infraestrutura de TI, de forma que foram indispensáveis para consolidação das seguintes ações estratégicas:
    - Melhorar a eficiência dos investimentos de TI;
    - Garantir a disponibilidade dos serviços de TIC essenciais às atividades educacionais e administrativas;
    - Garantir a estrutura de TIC apropriada às atividades educacionais e administrativas;

- Aprimorar continuamente a segurança das atividades do SENAC/TO;
- Aplicar a política de segurança da informação.

No entanto, a manutenção dos requisitos que compõem a segurança e os serviços de suporte para a solução de firewall são contratados por período definido e precisam ser renovados após encerrado o prazo de cobertura contratado.

Muito embora a solução continue em funcionamento após o encerramento do contrato de prestação dos serviços, ficar descoberta de atualizações de segurança bem como dos serviços de suporte em caso de problemas mais críticos não é prudente, ainda mais por um longo período, e, principalmente quando as atenções são direcionadas para os serviços providos e disponibilizados na rede do SENAC/TO.

Contudo, convém informar que os equipamentos adquiridos em 2019 são os que ainda compõem a solução de segurança do SENAC/TO, quais sejam: Firewall SonicWall NSA 3650 para o Datacenter principal do SENAC/TO e SonicWALL TZ's 500 para as demais Unidades Operativas, sendo que no cenário atual da instituição, é crescente a demanda pela oferta online de serviços com comunicação de alta velocidade com capacidade de prover dados, voz, vídeo e imagens com alto desempenho operacional, confiabilidade e tolerância a falhas. Neste sentido, a Coordenação Tecnologia da Informação no cumprimento de sua missão, buscando a melhoria da qualidade da rede de trafego de dados das unidades operativas, trabalhou na estruturação da rede Wi-fi com equipamentos corporativos com maior performance e também vem trabalhando na contratação de links de Internet mais velozes.

Uma vez que se amplia a velocidade dos links de comunicação e de Internet e na rede Wi-Fi, faz-se necessário também em investir em soluções de segurança do Tipo Firewall, com equipamentos que possuem capacidade para suportar o novo tráfego de dados entre as unidades administrativas e a internet. Logo, a contratação faz se necessária para que todas as unidades operativas que são interligados, possam usufruir dos benefícios oferecidos, pela maior qualidade, estabilidade e velocidade na transmissão de dados e internet, especialmente no que tange a eficiência no andamento dos procedimentos administrativos, e na prestação dos serviços online, de forma segura e protegida.

A modalidade de contratação apontada como melhor opção nos estudos técnicos realizados, é conhecida como Trade-Up, onde atrela a contratação à substituição dos atuais equipamentos por outros novos do mesmo fabricante, com melhor capacidade de processamento e performance, em uma relação custo x benefício vantajosa para o SENAC/TO. No entanto, caso a licitante vencedora seja fornecedor de outro fabricante, deverá atender as condições e especificações constantes deste Termo de Referência. Em ambas as situações, os equipamentos atuais permanecem em posse do SENAC/TO.

A modalidade de "Trade-Up" pretendida é ofertada por alguns fabricantes de solução de firewall (como a própria SonicWALL) e trará as seguintes vantagens para o SENAC/TO:

- A Licitante vencedora fará a substituição dos equipamentos em operação há mais de 3 anos, os quais ficariam obsoletos/ociosos em caso de novas aquisições.

- Caso a substituição seja por equipamentos do mesmo fabricante acrescentará ainda as seguintes vantagens:
  - Haverá facilidade e menor tempo na migração de toda solução de segurança para a nova plataforma de equipamentos devido a compatibilidade, sendo necessário somente um backup das configurações da estrutura atual e a restauração nos novos equipamentos;
  - O aproveitamento da expertise da equipe da Coordenação de Tecnologia da Informação (CTI) do SENAC/TO pela continuação da mesma tecnologia e estrutura de implementação da solução;
  - E em caso da Licitante vencedora ofertar solução de fabricante diferente, não haverá custo adicional, por parte do SENAC/TO, com a migração da solução, nem com capacitação da equipe da Coordenação de TI do SENAC/TO, visto que a Contratada terá que fornecer esses serviços sem custos adicionais, quando da substituição da Solução, conforme definido neste Termo de Referência;

Como forma de diminuir os custos administrativos com recorrentes contratações definimos que a contratação da Atualização da Solução de Firewall do SENAC/TO seja registrada com Garantia de 60 (sessenta) meses após a devida contratação e implementação.

3. DETALHAMENTO DO OBJETO, QUANTITATIVOS E VALORES MÁXIMOS ACEITOS

A Atualização da Solução de Firewall para segurança de perímetro da rede de dados do SENAC/TO, será composta da atualização do Software de Gerenciamento Centralizado, bem como da atualização dos modelos de appliances de firewall existentes, contemplando todas as licenças necessárias para os módulos de proteção, serviços de garantia e suporte, além de serviços de implantação e treinamento da solução. A tabela a seguir detalha os itens com seus respectivos quantitativos:

LOTE	ITEM	DESCRIÇÃO	QTD	LOCAL DE ENTREGA	VALOR UNITÁRIO	VALOR TOTAL
1	01	**Upgrade do Software de gerenciamento centralizado SonicWall GMS para SonicWall NSM** (conforme especificações dispostas no subitem 4.2) **OU SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO similar** (conforme especificações dispostas no subitem 5.2)	1	PALMAS – TO	R$ 71.263,74	R$ 71.263,74
	02	**Upgrade de appliance SonicWall NSA 3650 para SonicWall NSA 270**0 (conforme especificações dispostas no subitem 4.3) **OU SOLUÇÃO DE FIREWALL TIPO 01** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.4)	2	PALMAS – TO	R$ 58.472,47	R$ 116.944,94
	03	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** (conforme especificações dispostas no subitem 4.4) **OU SOLUÇÃO DE FIREWALL TIPO 02** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.5)	5	PALMAS – TO	R$ 19.625,54	R$ 98.127,70

	04	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** *(sem licenças de firewall),* (conforme especificações dispostas no subitem 4.5) **OU SOLUÇÃO DE FIREWALL TIPO 03** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.6)	1	PALMAS – TO	R$ 10.833,37	R$ 10.833,37
	05	**Serviços de Instalação e Configuração da Solução** (conforme especificações dispostas no subitem 4.6 para solução SonicWall ou 5.7 para outras soluções)	1	PALMAS - TO	R$ 23.033,00	R$ 23.033,00
	06	**Serviços de Treinamento Oficial (Voucher)** – (conforme especificações dispostas no subitem 4.7 para solução SonicWall e 5.8 para outras soluções)	4	PALMAS – TO	R$ 7.529,67	R$ 30.118,67
	07	**Serviços de Gerenciamento e Suporte Continuado - Solução de Firewall (Horas)** – (conforme especificações dispostas no subitem 4.8 para solução SonicWall e 5.9 para outras soluções)	360	PALMAS - TO	R$ 259,67	R$ 93.481,20
		TOTAL ESTIMADO DO LOTE				**R$ 443.802,62**

4. ESPECIFICAÇÕES TÉCNICAS

Nas especificações técnicas será descrito os requisitos mínimos exigidos para fornecimento da Atualização da Solução de Firewall do SENAC/TO, a qual compõe dos requisitos de segurança de firewall, serviços de suporte e atualização de hardwares.

4.1. Requisitos Gerais Obrigatórios

4.1.1. Os produtos ofertados deverão ser novos, de primeiro uso, estar em linha de produção e pertencer à linha corporativa de produtos comercializados pelo fabricante. Não serão aceitos equipamentos, softwares ou componentes que tenham sido descontinuados pelo fabricante ou que estejam listados para descontinuidade futura (end-of-life) na data da análise das propostas;

4.1.2. Responsabilizar-se totalmente pelo transporte, descarregamento e entrega dos equipamentos nos locais indicados pelo SENAC/TO, inclusive obedecendo o prazo de entrega estabelecido;

4.1.3. Substituir sem qualquer ônus para o SENAC/TO, os equipamentos eventualmente em desacordo com as especificações do objeto da licitação e consequentemente, com o constante da sua proposta, ou que, porventura, sejam entregues com defeitos e/ou imperfeições;

4.1.4. **O prazo de entrega não poderá ser superior a 45 (quarenta e cinco dias) consecutivos**, a partir do encaminhamento da Autorização de Fornecimento;

4.1.5. Todos os softwares fornecidos deverão estar em sua versão mais atual do fabricante, devendo constar na proposta comercial o seu PART NUMBER para efeito de comprovação;

4.1.6. Todos os cabos necessários à conexão entre os componentes objetos deste termo de referência deverão acompanhar o produto;

4.1.7. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da empresa proponente;

4.1.8. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características dos produtos ofertados, assim como informar marca e modelo dos mesmos. O simples fato de "COPIAR" e "COLAR" o descritivo contido no edital não será caracterizado como descritivo da proposta;

4.1.9. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades;

4.1.10. Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta;

4.1.11. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente;

4.1.12. No caso da fabricante SonicWall, atual fornecedor do SENAC-TO, os licitantes poderão optar pelo upgrade do software de gerenciamento e dos appliances de NGFW, desde que atendidas todas as especificações técnicas que se aplicam também aos demais fabricantes.

4.2. LOTE 1 - ITEM 01: UPGRADE DO SOFTWARE DE GERENCIAMENTO CENTRALIZADO SONICWALL GMS PARA SONICWALL NSM

4.2.1. Características Gerais:

4.2.1.1. Deverá ser fornecido o software de gerenciamento NSM (Network Security Manager), em substituição do software de gerenciamento GMS;

4.2.1.2. O software de gerenciamento deve vir licenciado para o quantitativo de 6 (seis) nós, atendendo assim o quantitativo de equipamentos ofertados;

4.2.1.3. O software de gerenciamento poderá ser ofertado em *appliance* físico ou virtual, como também em solução em nuvem;

4.2.1.4. Serão aceitas soluções de outros fabricantes, desde que, atendam as especificações mínimas descritas no tópico "ESPECIFICAÇÕES TÉCNICAS MÍNIMAS (PARA SOLUÇÕES DE OUTROS FABRICANTES)", item "SOFTWARE DE GERENCIAMENTO CENTRALIZADO" contidas neste termo de referência.

4.2.2. Garantia e Suporte

4.2.2.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

4.2.2.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

4.2.2.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

4.2.2.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE;

4.2.2.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

4.2.2.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

4.2.2.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7;

4.2.2.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

4.2.2.9. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta uma declaração do fabricante do equipamento garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital;

4.3. LOTE 1 - ITEM 02: UPGRADE DE APPLIANCE SONICWALL NSA 3650 PARA SONICWALL NSA 2700

4.3.1. Características Gerais:

4.3.1.1. Deverá ser fornecido o *appliance* Sonicwall NSA 2700, em substituição do *appliance* Sonicwall NSA 3650;

4.3.1.2. O *appliance* Sonicwall NSA 2700 deverá ser fornecido com as licenças necessárias para funcionamento dos módulos Comprehensive Anti-Spam, Capture Advanced Threat Protection , Content Filtering Services, Application Firewall Service, Gateway Anti-Virus, Application Firewall Service, Anti-Spyware e Intrusion Prevention, pelo período de 60 (sessenta) meses;

4.3.1.3. O appliance Sonicwall NSA2700 deverá ser fornecido com a licença do *software* Firewall, que permita montar um cenário, que garanta alta disponibilidade e possua o MAC virtual permitindo que a unidade de backup use o endereço MAC da unidade primária quando ocorrer um failover, isto se faz necessário para funcionamento da solução de Firewall;

4.3.1.4. O appliance Sonicwall NSA2700 deverá ser fornecido com fonte redundante;

4.3.1.5. Como características da modalidade *upgrade* de *hardware*, o fornecedor ao fornecer o *appliance* Sonicwall NSA2700, receberá em até 30 dias após a entrega do equipamento e em caráter definitivo, o *appliance* Sonicwall NSA3650 que é de propriedade do SENAC-TO. O SENAC-TO realizará a transferência de propriedade do equipamento para o fornecedor;

4.3.1.6. Serão aceitas soluções de outros fabricantes, desde que, atendam as especificações mínimas descritas no tópico "ESPECIFICAÇÕES TÉCNICAS MÍNIMAS (PARA SOLUÇÕES DE OUTROS FABRICANTES)", item "FIREWALL TIPO 1" contidas neste termo de referência.

4.3.2. Garantia e Suporte

4.3.2.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

4.3.2.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

4.3.2.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

4.3.2.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE;

4.3.2.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

4.3.2.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

4.3.2.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7;

4.3.2.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

4.3.2.9. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta

uma declaração do fabricante do equipamento garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital;

4.4. LOTE 1 - ITEM 03: UPGRADE DE APPLIANCE SONICWALL TZ 500 PARA SONICWALL TZ 370

4.4.1. Características Gerais:

4.4.1.1. Deverá ser fornecido o *appliance* Sonicwall TZ 370, em substituição do *appliance* Sonicwall TZ 500;

4.4.1.2. O *appliance* Sonicwall TZ 370 deverá ser fornecido com as licenças necessárias para funcionamento dos módulos Comprehensive Anti-Spam, Capture Advanced Threat Protection , Content Filtering Services, Application Firewall Service, Gateway Anti-Virus, Application Firewall Service, Anti-Spyware e Intrusion Prevention, pelo período de 60 (sessenta) meses;

4.4.1.3. Como características da modalidade *upgrade* de *hardware*, o fornecedor ao fornecer o *appliance* Sonicwall TZ 370, receberá em até 30 dias após a entrega do equipamento e em caráter definitivo, o *appliance* Sonicwall TZ 500 que é de propriedade do SENAC-TO. O SENAC-TO realizará a transferência de propriedade do equipamento para o fornecedor;

4.4.1.4. Serão aceitas soluções de outros fabricantes, desde que, atendam as especificações mínimas descritas no tópico "ESPECIFICAÇÕES TÉCNICAS MÍNIMAS (PARA SOLUÇÕES DE OUTROS FABRICANTES)", item "FIREWALL TIPO 2" contidas neste termo de referência.

4.4.2. Garantia e Suporte

4.4.2.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

4.4.2.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

4.4.2.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

4.4.2.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE.

4.4.2.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

4.4.2.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

4.4.2.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7;

4.4.2.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

4.4.2.9. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta uma declaração do fabricante do equipamento garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital;

4.5. LOTE 1 - ITEM 04: UPGRADE DE APPLIANCE SONICWALL TZ500 PARA SONICWALL TZ 370 (sem licenças de firewall).

4.5.1. Características Gerais:

4.5.1.1. Deverá ser fornecido o *appliance* Sonicwall TZ 370, em substituição do *appliance* Sonicwall TZ 500;

4.5.1.2. Como características da modalidade *upgrade* de *hardware*, o fornecedor ao fornecer o *appliance* Sonicwall TZ 370, receberá em até 30 dias após a entrega do equipamento e em caráter definitivo, o *appliance* Sonicwall TZ500 que é de propriedade do SENAC-TO. O SENAC-TO realizará a transferência de propriedade do equipamento para o fornecedor;

4.5.1.3. Serão aceitas soluções de outros fabricantes, desde que, atendam as especificações mínimas descritas no tópico "ESPECIFICAÇÕES TÉCNICAS MÍNIMAS (PARA SOLUÇÕES DE OUTROS FABRICANTES)", item "FIREWALL TIPO 3" contidas neste termo de referência.

4.5.2. Garantia e Suporte

4.5.2.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

4.5.2.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

4.5.2.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

4.5.2.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE;

4.5.2.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

4.5.2.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

4.5.2.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 8x5;

4.5.2.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

4.5.2.9. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta uma declaração do fabricante do equipamento garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital;

4.6. LOTE 1 - ITEM 05: SERVIÇOS DE INSTALAÇÃO

4.6.1. Requisitos Gerais

4.6.1.1. A CONTRATADA deverá realizar a instalação física e configuração lógica dos produtos que compõe este LOTE (NGFWs, Solução de Logs e Solução de Gerenciamento Centralizado), conforme quantitativo adquirido;

4.6.1.2. Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados;

4.6.1.3. Os serviços de implantação deverão ser executados presencialmente nas instalações da CONTRATANTE por técnico(s) da CONTRATADA capacitado(s) para tal;

4.6.1.4. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

4.6.1.5. Após e recebimento dos equipamentos e das licenças, a CONTRATANTE deverá definir, juntamente com a CONTRATADA, o cronograma de instalação e configuração dos mesmos, enviando a CONTRATADA, documento contendo informações de Data, Hora, Local, e soluções a serem instaladas;

4.6.1.6. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados;

4.6.1.7. Deverá ser agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

4.6.1.8. Deverá ser realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

4.6.1.9. Deverá ocorrer a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, por exemplo);

4.6.1.10. Deverá ser validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

4.6.1.11. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reunião de pré-projeto, devendo a CONTRADADA sugerir as configurações de acordo com normas e boas práticas, cabendo a CONTRATANTE a aceitação ou não;

4.6.1.12. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega das soluções. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

4.6.1.13. A CONTRATADA deverá realizar a instalação física e lógica “assistida” de todos os equipamentos, componentes e softwares, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

4.6.1.14. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

4.6.1.15. Após a conclusão dos serviços de instalação, o técnico da CONTRATADA deverá realizar o monitoramento da solução por pelo menos 03 (três) dias úteis, com acompanhamento da equipe da CONTRATANTE, a fim de identificar e sanar eventuais inconsistências;

4.6.1.16. Mesmo ao final da Implantação, a CONTRATANTE poderá solicitar, dentro de um período de 30 (trinta) dias e sem qualquer ônus, apoio à CONTRATADA para sanar dúvidas em relação funcionamento da solução;

4.6.1.17. Ao término da instalação, a CONTRATADA deverá entregar Caderno de Documentação “As Built” do Projeto, no qual conste todos os detalhes da instalação, tais como:

4.6.1.17.1. Descrição dos serviços implantados;

4.6.1.17.2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

4.6.1.17.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;
4.6.1.17.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;
4.6.1.17.5. Definição de responsabilidades;
4.6.1.17.6. Recursos de alta disponibilidade;
4.6.1.17.7. Procedimentos para abertura e atendimento a chamados;
4.6.1.17.8. Procedimentos de recuperação de equipamentos;
4.6.1.17.9. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;
4.6.1.17.10. Documentação dos processos de trabalho associados ao item;
4.6.1.17.11. Desenho dos racks onde estão instalados os equipamentos (bayface);
4.6.1.17.12. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);

4.6.2. Escopo dos Serviços de Implantação da Solução de Firewall:

4.6.2.1. Instalação e Configuração do Software de Gerenciamento Centralizado, quando aplicável;
4.6.2.2. Instalação das Soluções de Firewall, conforme contratado;
4.6.2.3. Configurar as Soluções de Firewall conforme segmentação de rede definida pela CONTRATANTE;
4.6.2.4. Atualização e aplicação de correções nas soluções de Firewall;
4.6.2.5. Implementação/migração de regras de Filtragem;
4.6.2.6. Implementação/migração de regras de NAT;
4.6.2.7. Implementação/migração de regras de QoS;
4.6.2.8. Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
4.6.2.9. Implementação de balanceamento e alta disponibilidade de links;
4.6.2.10. Integração com o Active Directory;
4.6.2.11. Tunning de configuração e regras de filtragem, removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados;
4.6.2.12. Testes gerais, validando o funcionamento das aplicações após a implementação dos Firewalls;

4.6.3. Local para realização dos serviços de Implantação:

4.6.3.1. A CONTRATANTE poderá contratar os serviços de Implantação para quaisquer uma de suas localidades;
4.6.3.2. As localidades para realização dos serviços são:

4.6.3.2.1. Unidade Operativa do Senac Araguaína – Gerencia da UOP. Telefone: 63 3321-5200. Endereço: Rua F, Qd AA, Lote 3, Setor George Yunes, CEP: 77.804-970, Araguaína - TO.
4.6.3.2.2. Unidade Operativa do Senac Gurupi – Gerencia da UOP. Telefone: 63 3301-4200. Endereço: Rua D, Quadra 10, Lotes 01 a 05, S/N, Bairro Engenheiro Waldir Lins. CEP: 77.423-030, Gurupi – TO
4.6.3.2.3. Centro de Educação Profissional do Senac em Palmas – Gerência do CEP: Telefone: 63 3219-1642. Endereço: Quadra 201 Norte, Avenida LO-04, Conjunto 03, Lotes 03 e 04, Sala 312, CEP 77.001-132, Palmas – TO
4.6.3.2.4. Administração Regional – Senac Tocantins. Telefone: 63 3219 1653. Endereço: Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomércio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas – TO
4.6.3.2.5. Unidade Operativa de Idiomas – Gerência da UOP. Telefone: 63 3219 1677. Endereço: Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomércio, 2º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas – TO.

4.7. LOTE 1 - ITEM 06: SERVIÇOS DE TREINAMENTO OFICIAL (VOUCHER)

4.7.1. Características Gerais

4.7.1.1. A CONTRATADA deverá fornecer voucher para Treinamento Oficial da solução de Firewall para equipe da técnica da CONTRATANTE, conforme os conteúdos mínimos indicados a seguir, com o intuito de assegurar a transferência de conhecimento para os Administradores de Redes e Analistas de Segurança da CONTRATANTE.

4.7.1.2. O treinamento deve ser na modalidade online, ou deverá ocorrer nas instalações da CONTRATANTE, na cidade de Palmas – TO;

4.7.1.3. O treinamento deverá ser ministrado por instrutor capacitado para tal, onde a contratada deverá comprovar no momento da execução do treinamento, através das certificações do fabricante da solução, a capacitação do instrutor;

4.7.1.4. As despesas decorrentes do serviço de treinamento como: confecção do material didático, deslocamentos, hospedagem e alimentação do instrutor designado pela CONTRATADA, serão de sua própria responsabilidade;

4.7.1.5. O treinamento deverá ser ministrado no idioma português, no entanto será aceito o fornecimento de materiais no idioma inglês;

4.7.1.6. O treinamento será de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e softwares da solução ofertada, em seus aspectos mais relevantes;

4.7.1.7. Para a consecução da parte prática do treinamento, deverão ser utilizados os equipamentos ofertados, além de todos os softwares que fizerem parte da solução, antes de suas ativações efetivas, fazendo a explanação das arquiteturas das soluções e seus componentes, rotinas de administração e gerenciamento do ambiente;

4.7.1.8. A CONTRATADA deverá emitir um certificado de participação do treinamento para cada aluno, mediante presença mínima em 75% do curso, comprovada por meio da lista de presença por ele assinada diariamente;

4.7.1.9. O treinamento deverá ser concluído em até 30 (trinta) dias após a assinatura do contrato;

4.7.1.10. O treinamento deverá ser aprovado por pelo menos 70% dos participantes do treinamento. Caso o treinamento seja considerado inadequado, a CONTRATADA deverá realizar novamente o serviço, às suas expensas, após realizar os ajustes necessários no material didático ou selecionar novo instrutor. Ocorrendo 2 (duas) rejeições do treinamento, a Administração poderá rescindir o contrato por inexecução;

4.7.1.11. Ao final do treinamento, os profissionais treinados deverão estar aptos a executar as seguintes atividades:

- 4.7.1.11.1. Instalação e configuração da Solução Firewall;
- 4.7.1.11.2. Implementação de regras de Filtragem;
- 4.7.1.11.3. Implementação de regras de NAT;
- 4.7.1.11.4. Implementação de regras de QoS;
- 4.7.1.11.5. Implementação de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
- 4.7.1.11.6. Implementação de balanceamento e alta disponibilidade de links;
- 4.7.1.11.7. Integração com o Active Directory;
- 4.7.1.11.8. Monitoramento dos serviços de redes;
- 4.7.1.11.9. Filtro de informações através de relatórios;
- 4.7.1.11.10. Atualização e aplicação de correções na solução de Firewall;
- 4.7.1.11.11. Backup e Restore do Solução de Firewall;

4.7.1.12. Ao final do treinamento todos os alunos instruídos deverão receber as provas para certificação oficial do fabricante sem custo adicional ao projeto;

4.7.1.13. A carga horária total do treinamento deverá ser de no mínimo 16 (dezesseis) horas e o voucher ofertado deverá ser individual para cada participante;

4.8. LOTE 1 – ITEM 07: SERVIÇOS DE GERENCIAMENTO E SUPORTE CONTINUADO - SOLUÇÃO DE FIREWALL (HORAS)

4.8.1. Características Gerais

4.8.1.1. Será realizado como prestação de serviço, sob demanda, com banco de horas;

4.8.1.2. O saldo do banco de horas terá validade de 12 (doze) meses, sendo descontado e pago mensalmente o valor correspondente às horas usadas do banco;

4.8.1.3. O serviço poderá ser realizado remotamente (através de software próprio da CONTRATADA) ou presencialmente, conforme necessidade para a solução da requisição/incidente;

4.8.1.4. A CONTRATADA poderá disponibilizar, no ato de abertura do incidente ou requisição pela CONTRATANTE, dependendo do nível de criticidade do atendimento, que o atendimento seja feito de maneira presencial ou de maneira remota;

4.8.1.5. O atendimento deverá ser realizado por profissionais que possuam experiência comprovada para o atendimento completo das soluções. Para tal comprovação, deverá ser apresentado, no ato da assinatura do contrato, pela CONTRATADA ao menos 1 (um) profissional certificado pelo fabricante da solução proposta;

4.8.1.6. A solicitação do serviço será feita pelo CONTRATANTE, através de chamado (eletrônico ou telefônico), e-mail ou documento oficial, expedido ao prestador;

4.8.1.7. O período de abertura e resolução dos chamados será contabilizado no regime 24x7 (24 horas e 7 dias da semana);

4.8.1.8. Os prazos de atendimento deverão obedecer aos níveis de serviço conforme criticidade, descritas no item “Os tipos de criticidade e o tempo de atendimento (SLA)” mais adiante;

4.8.1.9. A CONTRATADA deverá dispor de telefone em DDD (63) ou número 0800 ou permitir ligações à cobrar para a abertura de chamados;

4.8.1.10. A CONTRATADA deverá disponibilizar e-mail para a abertura de chamados;

4.8.1.11. O acesso ao ambiente (incluindo o caso de atendimento remoto) será supervisionado por profissional da CONTRATANTE. A CONTRATADA obriga-se a respeitar as políticas de segurança e de sigilo impostas pela CONTRATANTE;

4.8.1.12. Será realizado o gerenciamento, monitoramento e suporte diário do ambiente, com desconto no banco de horas de **15h (quinze horas)** para cada mês. É necessário a apresentação de relatórios fixos mensal com no mínimo:

- 4.8.1.12.1. Número de chamados abertos e estatísticas de tipo, criticidade, tempo de resolução, entre outros filtros;
- 4.8.1.12.2. Tempo médio de atendimento de chamados;
- 4.8.1.12.3. Usuários com maior atividade permitida (pelo endereço IP/nome do usuário);
- 4.8.1.12.4. Domínios mais acessados;
- 4.8.1.12.5. Categorias de site mais acessadas;
- 4.8.1.12.6. Aplicações mais acessadas;
- 4.8.1.12.7. Categorias de aplicações mais acessadas;
- 4.8.1.12.8. Aplicações bloqueadas;
- 4.8.1.12.9. Categorias de aplicações mais bloqueadas;
- 4.8.1.12.10. Protocolos IP com maior atividade (entrada e saída);
- 4.8.1.12.11. Relatório de malwares detectados;
- 4.8.1.12.12. Relatório de tentativas de intrusão.

4.8.1.13. Os relatórios acima não serão descontados das horas disponíveis do banco de horas além do limite de 15h (quinze horas) mensais. Na data de entrega da instalação do projeto, será realizada reunião para alinhamento dos relatórios mensais fixos;

4.8.1.14. Novos relatórios poderão ser solicitados pela CONTRATANTE, sem adição de custos ou consumo de horas adicionais, desde que os dados sejam relativos ao sistema de gerenciamento de chamados ou que sejam variações dos relatórios fixos listados anteriormente;

4.8.1.15. Caso seja necessário a criação de rotina automatizada ou a criação de qualquer procedimento para a coleta de dados para a confecção de relatório fixo diverso aos já elencados, será acordado entre as partes o desconto de horas a ser realizado pelos ajustes;

4.8.1.16. As atividades que compreendem o atendimento serão:

4.8.1.16.1. Dúvidas técnicas sobre a configuração dos componentes de hardware e software que compõem o projeto, ou outras;

4.8.1.16.2. Atualizações de firmwares/microcódigos de todos os componentes de hardware e software da solução;

4.8.1.16.3. Testes de performance, segurança e disponibilidade dos serviços;

4.8.1.16.4. Inclusão/exclusão/alteração de regras, nos equipamentos Firewall, com análise crítica a fim de garantir a gestão de mudanças no ambiente da CONTRANTE;

4.8.1.16.5. Identificar brechas e vulnerabilidades na configuração de regras implantadas e propor, de forma contínua, melhorias na proteção do ambiente, sempre que identificado a necessidade;

4.8.1.16.6. Monitoramento do acesso não intrusivo de conectividade e consumo de banda do acesso, sem visibilidade dos dados trafegados pela rede;

4.8.1.16.7. Realização de backup periódico das configurações das soluções;

4.8.1.16.8. Restauração das configurações das soluções, quando houver necessidade;

4.8.1.16.9. Criar regras de QoS para controle de tráfego de aplicações, quando aplicável;

4.8.1.16.10. Realizar análise e diagnóstico do ambiente para resolução de problemas;

4.8.1.16.11. Resolução de problemas do ambiente com base nas criticidades mencionadas no acordo de nível de serviço;

4.8.1.16.12. Abrir e acompanhar os chamados de suporte junto aos fabricantes das soluções, quando for o caso;

4.8.1.17. A CONTRATADA deverá monitorar remotamente os eventos abaixo relacionados e alertar a CONTRANTE para as providências cabíveis:

4.8.1.17.1. Intrusões detectadas pelos módulos de IPS e antivírus do equipamento de Firewall UTM ofertado;

4.8.1.17.2. Indisponibilidade do cluster, quando houver, de Firewall;

4.8.1.17.3. Indisponibilidade de VPN;

4.8.1.17.4. Indisponibilidade dos links de Internet;

4.8.1.17.5. Sobrecarga de processamento;

4.8.1.18. Os tipos de criticidade e o tempo de atendimento (SLA) serão:

4.8.1.18.1. Criticidade 1 – Falha de hardware ou software que não comprometa o funcionamento do ambiente, que não gera indisponibilidade dos serviços, mas que alarma ou sinaliza falha em componentes físicos ou virtuais, falha em rotinas ou necessidades de atualizações;

4.8.1.18.2. SLA Criticidade 1 - Atendimento em até 16 horas úteis (8x5) após abertura do chamado;

4.8.1.18.3. Criticidade 2 – Falha de hardware ou software que não comprometa o funcionamento do ambiente e serviços, porém, que aciona componentes e funcionalidades de redundância, expondo o ambiente à um possível problema e parada em caso de nova falha;

4.8.1.18.4. SLA Criticidade 2 – Atendimento em até 10 horas úteis (8x5) após abertura do chamado;

4.8.1.18.5. Criticidade 3 - Falha de hardware ou software que comprometa o funcionamento do ambiente e serviços, gerando indisponibilidade completa ou parcial de qualquer serviço crítico ou que comprometa a imagem do órgão e de suas atividades e colaboradores;

4.8.1.18.6. SLA Criticidade 3 – Atendimento em até 8 horas (24x7) após abertura do chamado;

4.8.1.19. O não atendimento dos prazos do nível de serviço ensejará no desconto percentual do pagamento a ser realizado pelo chamado aberto. O desconto será executado no fim do ciclo mensal, e será calculado da seguinte forma:

$$Tempo\ excedido\ em\ horas = T.Exc\ (arendado\ para\ maior\ inteiro)$$

$$Tempo\ máximo, em\ horas, para\ atendimento\ do\ chamado\ (por\ criticidade) = SLA$$

$$\boldsymbol{Desconto} = 25\% * \left(\frac{T.Exc}{SLA}\right)$$

4.8.1.20. O desconto máximo é limitado ao valor de 100% das horas demandadas para resolução do chamado que não atendeu ao prazo do SLA;

4.8.1.21. A CONTRATANTE poderá, justificadamente, prorrogar o prazo de atendimento das solicitações e chamados, caso julgue necessário ou pertinente;

5. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS (PARA SOLUÇÕES DE OUTROS FABRICANTES)

5.1. Requisitos Gerais Obrigatórios

5.1.1. Os produtos ofertados deverão ser novos, de primeiro uso, estar em linha de produção e pertencer à linha corporativa de produtos comercializados pelo fabricante. Não serão aceitos equipamentos, softwares ou componentes que tenham sido descontinuados pelo fabricante ou que estejam listados para descontinuidade futura (end-of-life) na data da análise das propostas;

5.1.2. Todos os softwares fornecidos deverão estar em sua versão mais atual do fabricante, devendo constar na proposta comercial o seu PART NUMBER para efeito de comprovação;

5.1.3. Todos os cabos necessários à conexão entre os componentes objetos deste termo de referência deverão acompanhar o produto;

5.1.4. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da empresa proponente;

5.1.5. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características dos produtos ofertados, assim como informar marca e modelo dos mesmos. O simples fato de “COPIAR” e “COLAR” o descritivo contido no edital não será caracterizado como descritivo da proposta;

5.1.6. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades;

5.1.7. Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta;

5.1.8. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente;

5.2. LOTE 1 - ITEM 01: SOFTWARE DE GERENCIAMENTO CENTRALIZADO

5.2.1. Características Gerais:

5.2.1.1. Poderá ser composto de appliance ou máquina virtual ou solução em nuvem, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade. A solução deverá ser do mesmo fabricante do equipamento de firewall;

5.2.1.2. Deve ser separada do gateway de segurança e gerenciar políticas de segurança de todos os firewalls;

5.2.1.3. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados;

5.2.1.4. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

5.2.1.5. A solução deve permitir controle granular do acesso dos administradores, utilizando controle de acesso do tipo RBAC (Role based access control), aumentando a segurança e integridade da plataforma;

5.2.1.6. A solução deve permitir que os administradores façam autenticação no console utilizando no mínimo dois fatores de autenticação, 2FA (two factors authentication);

5.2.1.7. A solução deve fornecer uma ferramenta de gestão centralizada capaz de reunir todos os equipamentos sob uma única interface gráfica, possibilitando o gerenciamento unificado de políticas e regras de todos os firewalls ofertados;

5.2.1.8. A solução deve permitir tecnologia de "Zero touch" para os dispositivos de NGFW;

5.2.1.9. A solução deve possuir tela situacional com todo o inventário de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou offline;

5.2.1.10. Deve ser possível visualizar a último horário de comunicação entre o firewall e a gerência, onde deve ser informado ao administrador, pela console, se a configuração do dispositivo está sincronizada ou não;

5.2.1.11. A solução deve oferecer as funcionalidades de backup de configurações dos equipamentos gerenciados, permitindo que o administrador possa agendar procedimentos de backup em dias ou horários específicos e exportá-los e acordo com o agendamento;

5.2.1.12. A solução deve oferecer as funcionalidades de backup e agendamento de arquivo com informações técnicas do dispositivo para utilização do suporte técnico do fabricante;

5.2.1.13. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;

5.2.1.14. Deverá permitir atualizar o sistema operacional dos equipamentos gerenciados, onde deverá ser possível criar agendamento para a atualização;

5.2.1.15. Deve centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

5.2.1.16. A solução deve possuir Dashboard com sumario de alertas e informação de equipamentos com licenciamento expirando;

5.2.1.17. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo;

5.2.1.18. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência;

5.2.1.19. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN;

5.2.1.20. A solução de gerência deve prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de políticas e configuração de todos os firewalls em uma única sessão, evitando qualquer tipo de retrabalho de configuração e aplicação de regra;

5.2.1.21. A solução deve permitir a criação de modelos de configuração ou "Templates" para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls.

5.2.1.22. Os modelos de configuração ou "templates" devem suportar configurações de interfaces físicas ou virtuais.

5.2.1.23. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez;

5.2.1.24. A solução deverá contar com tela situacional para a gestão de configurações e mudanças das políticas de segurança, onde deve permitir visualizar as alterações feitas pelos administradores, como exemplo, mas não limitado a: data e horário da aplicação das alterações, quantidade de dispositivos afetados pelas alterações, sumario da alteração, status de sucesso ou insucesso da alteração e comentários deixados pelo administrador durante a alteração das políticas;

5.2.1.25. Deverá suportar API (interface de programação de aplicativo) RESTful para criação de scripts personalizados para gerenciar e configurar e os equipamentos de acordo com a necessidade de customização do administrador;

5.2.1.26. Para cada alteração configurada nos firewalls, o sistema de gerenciamento centralizado deverá possibilitar a visualização e o download dos comandos enviados ao gateway, em formato de API, para o uso do administrador;

5.2.1.27. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas;

5.2.1.28. De forma centralizada deve permitir gerenciar, mas não limitado a, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e anti-malware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de políticas de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

5.2.1.29. Registrar em log de auditoria as ações dos usuários administradores, registrando todas as alterações realizadas em uma política de segurança, permitindo a identificação do responsável pela mudança, o horário e a origem;

5.2.1.30. A solução deverá permitir o rastreamento e auditoria das alterações de políticas e configurações de no mínimo dos últimos 20 dias;

5.2.1.31. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria;

5.2.1.32. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente;

5.2.1.33. Permitir a criação de janela de mudança podendo executar regras imediatamente ou criar um agendamento;

5.2.1.34. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente de segurança da informação do órgão;

5.2.1.35. A funcionalidade de Workflow deve permitir o administrador definir se o processo de aprovação por um usuário será completo ou parcial, para que possa ser definido se o processo de aprovação terá apenas um aprovador ou vários aprovadores;

5.2.1.36. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada;

5.2.1.37. A funcionalidade de Workflow deve permitir o administrador criar de grupos de aprovação com os aprovadores e e-mails que receberão a notificação de pendência de aprovação;

5.2.1.38. A Solução deverá permitir visualizar a topologia na qual determinado firewall está inserida;

5.2.1.39. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls;

5.2.1.40. A solução de gerenciamento centralizado deve estar licenciada para suportar o gerenciamento de todos appliances de Firewall (com exceção do Item 04 “FIREWALL TIPO 3”), num total de 6 nós;

5.2.2. Características de Relatórios:

5.2.2.1. Deverá receber suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar reports;

5.2.2.2. A solução deverá prover relatórios com no mínimo histórico de 365 dias;

5.2.2.3. A solução deverá prover relatórios referente as atividades dos usuários;

5.2.2.4. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações, nome da aplicação, quantidade de conexões e percentual que a aplicação representa do tráfego da rede, quantidade de Megabytes trafegados, quantidades de bloqueios que existe para a Aplicação, nível de risco e categoria da aplicação;

5.2.2.5. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações, nome do usuário, quantidade de conexões e percentual que tráfego do usuário representa na rede, quantidade de Megabytes trafegados, quantidades de bloqueios de tráfego para o usuário e quantidade de vírus/spyware/intrusões encontrado no tráfego dos usuários;

5.2.2.6. Caso o administrador não habilitado a funcionalidade de identificação do usuário, a solução deverá identificar as informações acima como usuário desconhecido;

5.2.2.7. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações: endereço IP, quantidade de conexões e percentual que tráfego que o IP representa na rede, quantidade de Megabytes trafegados, quantidades de bloqueios de tráfego para o endereço IP e quantidade de vírus/spyware/intrusões encontrado no tráfego;

5.2.2.8. A solução deverá prover relatórios referente aos acessos geográficos, com no mínimo as seguintes informações: país de origem/destino do tráfego, quantidade de conexões e percentual que tráfego que do país representa na rede, quantidade de Megabytes trafegados do todo, quantidade de Megabytes enviados e recebidos por país.

5.2.2.9. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes as categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede;

5.2.2.10. A solução deverá permitir criar agendamentos para geração automática de relatórios no formato PDF, possibilitando o envio dos relatórios agendados via e-mail;

5.2.2.11. A solução deve possuir tela situacional com informações referente a geração dos relatórios agendados, informando se houve sucesso, falha ou se existe relatórios em progresso;

5.2.2.12. A solução deverá arquivar os relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF;

5.2.3. Garantia e Suporte

5.2.3.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

5.2.3.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

5.2.3.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

5.2.3.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE;

5.2.3.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

5.2.3.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

5.2.3.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7;

5.2.3.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

5.2.3.9. Devido à necessidade de atendimento de suporte à CONTRATANTE, caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta uma declaração do fabricante do equipamento garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital;

5.3. LOTE 1 - ITENS 02, 03 e 04 - SOLUÇÃO DE FIREWALL TIPO 1, TIPO 2 e TIPO 3 (CARACTERÍSTICAS COMUNS A TODOS)

5.3.1. Características Gerais

5.3.1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL;

5.3.1.2. Define-se o termo "appliance" como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;

5.3.1.3. O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, de um NGFW não sendo baseado em plataforma X86 ou equivalente;

5.3.1.4. O appliance deve possuir memória flash com capacidade suficiente para armazenamento do sistema operacional do NGFW. Não serão aceitos Sistemas Operacionais do Tipo "Harderizado";

5.3.1.5. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de "appliance" que utilizam hardware e software de fabricantes diferentes;

5.3.1.6. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões;

5.3.1.7. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW;

5.3.1.8. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

5.3.1.9. Devem ser fornecidas todas as licenças necessárias para o funcionamento das funcionalidades de Filtro de Conteúdo Web, IPS, Gateway Antivírus, Controle de Aplicações e Proteção contra Ameaças Avançadas (com exceção do Item 04 "FIREWALL TIPO 3");

5.3.1.10. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP;

5.3.1.11. As interfaces de rede do appliance deverão ser configuráveis pelo administrador do firewall para atender os segmentos de segurança e rede para:

5.3.1.11.1. Segmento WAN, ou externo;

5.3.1.11.2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;

5.3.1.11.3. Segmento LAN ou rede interna;

5.3.1.11.4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

5.3.1.11.5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;

5.3.1.11.6. Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos;

5.3.1.12. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL/TSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante, verificado possíveis ameaças e então re-criptografado e enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. O recurso poderá ser fornecido através de uma licença adicional ao equipamento;

5.3.1.13. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3;

5.3.1.14. Não possuir limitação de segmentos de rede a serem protegidos;

5.3.1.15. Deve implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 (três) servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

5.3.1.16. Possibilitar o controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

5.3.1.17. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.

5.3.1.18. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/Anti-Spyware;

5.3.1.19. Possibilitar o controle do tráfego para os protocolos GRE, H323 Full v1-5, suporte a tecnologia a gatekeeper, SIP e IGMP baseados nos endereços origem e destino da comunicação;

5.3.1.20. Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço;

5.3.1.21. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

5.3.1.22. Prover mecanismos de proteção contra ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com “malwares”. O recurso deverá prevenir ataques e analises aos seguintes endereços:

5.3.1.22.1. Node-local address 127.0.0.1;

5.3.1.22.2. Link-local address 169.254.0.0/24;

5.3.1.22.3. Multicast address 224.0.0.0/24;

5.3.1.22.4. Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN;

5.3.1.23. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem, subrede de origem e destino;

5.3.1.24. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;

5.3.1.25. Deve suportar DHCP relay;

5.3.1.26. Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como IP Helper suportando os protocolos e portas:

5.3.1.26.1. Time service - UDP porta 37;

5.3.1.26.2. DNS - UDP porta 53;

5.3.1.26.3. DHCP - UDP portas 67 e 68;

5.3.1.26.4. Net-Bios DNS - UDP porta 137;

5.3.1.26.5. Net-Bios Datagram - UDP porta 138;

5.3.1.26.6. Wake On LAN - UDP porta 7 e 9;

5.3.1.26.7. mDNS - UDP porta 5353;

5.3.1.27. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

5.3.1.28. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

5.3.1.29. Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso;

5.3.1.30. Possuir suporte ao protocolo SNMP versões 2 e 3;

5.3.1.31. Possuir suporte a log via syslog;

5.3.1.32. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

5.3.1.33. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

5.3.1.34. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão;

5.3.2. Características Anti-Malware:

5.3.2.1. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream, permitindo o bloqueio de malwares (vírus, worms, spyware e etc);

5.3.2.2. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;

5.3.2.3. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

5.3.2.4. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 "FIREWALL TIPO 3");

5.3.3. Características IPS / IDS:

5.3.3.1. Possuir Mecanismo de IPS / IDS, baseado em assinatura, com suporte a pelo menos 3.000 (três mil) assinaturas de ataques, aplicações ou serviços, completamente integrados ao Firewall;

5.3.3.2. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;

5.3.3.3. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

5.3.3.4. Possuir capacidade de remontagem de pacotes para identificação de ataques;

5.3.3.5. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas à webserver para que seja usado para proteção específica de Servidores Web;

5.3.3.6. 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;

5.3.3.7. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

5.3.3.8. Detectar e bloquear a origem de portscans;

5.3.3.9. Reconhecimento de padrões;

5.3.3.10. Análise de protocolos;

5.3.3.11. Detecção de anomalias;

5.3.3.12. Detecção de ataques de RPC (Remote procedure call);

5.3.3.13. Proteção contra ataques DNS (Domain Name System);

5.3.3.14. Proteção contra ataques de ICMP (Internet Control Message Protocol);

5.3.3.15. Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;

5.3.3.16. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

5.3.3.17. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 "FIREWALL TIPO 3");

5.3.4. Filtro de Conteúdo Web:

5.3.4.1. Possuir módulo integrado ao mesmo NGFW para classificação de páginas web com no mínimo 50 (cinquenta) categorias distintas pré-definidas, com mecanismo de atualização e consulta automática;

5.3.4.2. Permitir a classificação dinâmica de sites web, URLs e domínios;

5.3.4.3. Das categorias pré-definidas, devem existir pelo menos as seguintes: violência, nudismo, roupas intimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar, hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting;

5.3.4.4. Deve permitir a criação de no mínimo 5 (cinco) novas categorias personalizadas;

5.3.4.5. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

5.3.4.6. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

5.3.4.7. Capacidade de submissão de novos sites através de portal web ou suporte do Fabricante;

5.3.4.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

5.3.4.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

5.3.4.10. O administrador poderá adicionar filtros por palavra-chave de modo específico;

5.3.4.11. Permitir aplicação da política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

5.3.4.12. 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;

5.3.4.13. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

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

5.3.4.15. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas, assim como, lista negra;

5.3.4.16. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem e por subrede de origem;

5.3.4.17. Deverá permitir o bloqueio Web através de senha pré configura pelo administrador;

5.3.4.18. Deverá permitir criar política de confirmação de acesso;

5.3.4.19. Deverá bloquear sites embarcados dentro outros sites como por exemplo translate.google.com.br;

5.3.4.20. Possibilitar a customização de mensagens de bloqueio para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança interna;

5.3.4.21. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças para quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 “FIREWALL TIPO 3”);

5.3.5. Controle de aplicações:

5.3.5.1. Reconhecer no mínimo aplicações como: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

5.3.5.2. A solução deve possuir a capacidade de identificar pelo menos 1.500 (mil e quinhentas) aplicações para controle, bloqueio e agendamento deste recurso por usuário e grupo de usuário;

5.3.5.3. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos e;

5.3.5.4. Devem ser aplicados por usuário e por grupo e;

5.3.5.5. Associado sua ação, políticas de horários e dias da semana e;

5.3.5.6. Podem ser associados a endereçamento IP baseados em sub-redes e;

5.3.5.7. Permitindo a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime;

5.3.5.8. Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;

5.3.5.9. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada;

5.3.5.10. Controlar o uso dos serviços de Instant Messengers, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

5.3.5.11. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 HTTP, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

5.3.5.12. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate, dentre outros;

5.3.5.13. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 “FIREWALL TIPO 3”);

5.3.6. Proteção Contra Ameaças Avançadas:

5.3.6.1. A solução deverá prover as funcionalidades, através de serviço de sandbox local ou em nuvem, de inspeção de tráfego de entrada e saída de malwares não conhecidos (ameaças de dia zero) ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

5.3.6.2. Este mecanismo deve propiciar um ambiente isolado/controlado onde arquivos suspeitos ou aplicativos sejam executados, examinados e sondados antes que passem através do firewall para a rede interna;

5.3.6.3. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

5.3.6.4. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

5.3.6.5. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS;

5.3.6.6. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TSL e SSH;

5.3.6.7. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

5.3.6.8. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

5.3.6.9. O serviço deve suportar análise vários tipos e tamanhos de arquivos, incluindo programas executáveis, DLL, PDFs, ZIP, documentos do MS Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos, JAR e APK no ambiente controlado;

5.3.6.10. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

5.3.6.11. Deve possibilitar aos administradores personalizar a proteção, selecionando ou excluindo arquivos para serem enviados para a análise por tipo de arquivo, tamanho do arquivo, remetente, destinatário ou protocolo;

5.3.6.12. Deve possibilitar aos administradores enviarem arquivos manualmente para análise;

5.3.6.13. Para os arquivos enviados para o serviço avançado de proteção para análise, deve-se realizar o bloqueio de arquivos suspeitos até o veredicto, evitando que arquivos potencialmente maliciosos entrem na rede;

5.3.6.14. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

5.3.6.15. Quando um arquivo for identificado como mal-intencionado, deve-se ser gerada uma assinatura imediatamente e disponibilizá-la para os firewalls, para evitar ataques subsequentes;

5.3.6.16. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;

5.3.6.17. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

5.3.6.18. A análise em nuvem ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações, processos, registros são afetadas pelo malware, gerar assinaturas de Antivírus e Antispyware baseadas no hash da ameaça automaticamente, definir endereços e protocolos utilizados pela ameaça, mostrando a quantidade de dados trafegados nas conexões abertas pelo malware, a ferramenta deve prover e prover Informações sobre o usuário infectado (seu endereço IP ou seu login de rede);

5.3.6.19. Caso esta funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 “FIREWALL TIPO 3”);

5.3.7. Características de VPN:

5.3.7.1. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel) de acordo com as RFCs 2401 a 2412, de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

5.3.7.2. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;

5.3.7.3. Suportar os algoritmos de criptografia 3DES, AES 128 e AES 256;

5.3.7.4. Suportar os algoritmos Hash SHA-1, SHA-256 e SHA-384;

5.3.7.5. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);

5.3.7.6. Suportar autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

5.3.7.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android;

5.3.7.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico;

5.3.7.9. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

5.3.7.10. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

5.3.7.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;

5.3.7.12. Deve possuir interoperabilidade com pelo menos os seguintes fabricantes: Cisco, Check Point, Fortinet, Juniper, Palo Alto Networks e SonicWall;

5.3.8. Características de NAT:

5.3.8.1. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;

5.3.8.2. Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI.

5.3.8.3. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;

5.3.8.4. Possuir mecanismo que permita conversão de portas (PAT);

5.3.8.5. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

5.3.8.6. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

5.3.9. Características de QoS:

5.3.9.1. Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;

5.3.9.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade e gerência de congestionamento;

5.3.9.3. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

5.3.9.4. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

5.3.9.5. Limitar individualmente a banda utilizada por aplicação;

5.3.9.6. Deverá controlar (limitar) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

5.3.9.7. Deverá controlar (limitar) individualmente a banda utilizada por subrede de origem e destino;

5.3.9.8. Deverá controlar (limitar) individualmente a banda utilizada por endereço IP de origem e destino.

5.3.10. Características de Roteamento:

5.3.10.1. Suportar os protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP, sendo possível a configuração pela interface gráfica para, pelo menos, RIP, RIPng e OSPF;

5.3.10.2. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;

5.3.10.3. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação;

5.3.10.4. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

5.3.10.5. Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;

5.3.10.6. Possibilitar o roteamento de tráfego IGMP versão 3 em suas interfaces e zonas de segurança.

5.3.11. Características de Gerenciamento Nativo:

5.3.11.1. Fornecer gerência remota, com interface gráfica WEB segura nativa, utilizando o protocolo HTTPS;

5.3.11.2. Possuir interface CLI (orientada a linha de comando) segura para a administração do firewall a partir do console com conexão via protocolo SSH;

5.3.11.3. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

5.3.11.4. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

5.3.11.5. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

5.3.11.6. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica;

5.3.11.7. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional;

5.3.11.8. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração;

5.3.11.9. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

5.3.11.10. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o NGFW remotamente através da interface gráfica;

5.3.11.11. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW, bem como possibilitar a remoção de qualquer uma destas sessões ou conexões;

5.3.11.12. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;

5.3.11.13. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

5.3.11.14. Permitir, através da interface gráfica remota, a visualização em forma gráfica e em tempo real das estatísticas do uso de CPU e tráfego de rede em todas as interfaces do NGFW;

5.3.11.15. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

5.3.11.16. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento;

5.3.11.17. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

5.3.11.18. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6;

5.3.11.19. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

5.3.11.20. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web);

5.3.11.21. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

5.3.11.22. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;

5.3.11.23. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android;

5.3.11.24. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB;

5.3.11.25. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW;

5.3.11.26. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

5.3.11.27. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW;

5.3.11.28. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS;

5.3.11.29. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações;

5.3.12. Características de Alta Disponibilidade:

5.3.12.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Ativo ou Ativo/Standby, com as implementações de Fail Over e Load Balance, sendo que na implementação de Load Balance o estado das conexões e sessões TCP e UDP deve ser replicado sem restrições de serviços como, por exemplo, tráfego multicast;

5.3.12.2. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos reiniciem após qualquer modificação de parâmetro/configuração seja realizada pelo administrador;

5.3.12.3. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

5.3.12.4. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover;

5.3.12.5. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

5.3.12.6. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

5.3.12.7. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante;

5.3.12.8. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;

5.3.13. Autenticação:

5.3.13.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

5.3.13.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API;

5.3.13.3. Quando integrado com Microsoft Active Directory, deve reconhecer grupos de usuários cadastrados e prover funcionalidade de identificação transparente de usuários;

5.3.13.4. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

5.3.13.5. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

5.3.13.6. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser;

5.3.13.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW;

5.3.13.8. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

5.3.13.9. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;

5.3.13.10. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no NGFW sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2012/2016/2019 com AD;

5.3.14. Módulo de Logs e Relatórios Analíticos

5.3.14.1. A solução de NGFW a ser entregue, deverá possuir módulo de gerenciamento de logs e relatórios, podendo este ser ofertada em appliance separado do próprio fabricante da solução de segurança para esta finalidade ou ambiente virtualizado, também do próprio fabricante, compatível com VMware ESXi. Também será aceito soluções em nuvem do mesmo fabricante da solução, devendo ser ofertada com mesmo período de licenciamento e suporte solicitação para o equipamento de NGFW;

5.3.14.2. Através do módulo de Gerenciamento de Logs e Relatórios deve ser possível coletar e armazenar fluxos e dados de log do NGFW e usá-los para análise de dados e relatórios analíticos;

5.3.14.3. Deve suportar o recebimento de logs dos equipamentos NGFW através do protocolo Syslog ou protocolo proprietário do fabricante, possibilitando o armazenamento de longo prazo de logs em uma única instância, ou seja, promover o recebimento e gerenciamento dos logs de vários appliances de forma centralizada;

5.3.14.4. Deve possuir Dashboard que indica informações sobre:

5.3.14.4.1. Aplicações e categorias de URL's mais acessadas;

5.3.14.4.2. Principais ameaças detectadas;

5.3.14.4.3. Número de vírus, intrusões, spyware, botnets, detectados;

5.3.14.4.4. Informações de conexões, tais como: total de conexões e taxa de conexões por segundo;

5.3.14.4.5. Informações sobre taxa de uso de banda e total de dados transferidos;

5.3.14.5. Deve possuir funcionalidade de relatórios sumarizados que forneçam um resumo executivo dos vários tipos de dados que estão sendo rastreados pelo NGFW, onde seja possível iniciar a verificação do funcionamento geral, bem como possuir relatórios detalhados;

5.3.14.6. Deve suportar a visualização e geração de no mínimo os seguintes relatórios:

5.3.14.6.1. Ameaças (vírus, spyware, botnets, intrusões, etc) que foram detectadas e bloqueadas;

5.3.14.6.2. Aplicativos, bem como a integridade dos mesmos, que passam pelo NGFW;

5.3.14.6.3. Usuários conectados ao sistema, onde seja possível identificar as transações e atividades a nível de usuário;

5.3.14.6.4. Acesso/conexões com base em categorias web, sendo possível realizar filtros por categoria;

5.3.14.6.5. Conexões com base no endereço IP e localidade de Origem/Destino;

5.3.14.7. Através da console deve ser possível verificar as atividades de navegação na Web de endereços IPs específicos, onde seja possível visualizar dados da sessão, tais como:

5.3.14.7.1. Data/hora de acesso;

5.3.14.7.2. Domínio e categoria da URL acessada

5.3.14.7.3. Endereço IP, Porta, MAC, Interface, Gateway e País do iniciador da conexão;

5.3.14.7.4. Informações sobre ameaça caso detectada;

5.3.14.7.5. Ação realizada pelo NGFW;

5.3.14.8. Deve possibilitar, através da console, monitorar: aplicações, usuários, atividades de navegação, Origens e Destinos de conexões, ameaças identificadas;

5.3.14.9. Deve suportar navegação “drill down” para realização de análise investigativas e obtenção de informações a rede, acesso do usuário, conectividade, uso de aplicativos, perfis de ameaças e outros dados relacionados ao NGFW.

5.3.14.10. Caso esta solução/funcionalidade seja baseada em assinatura no formato subscrição, deverão ser fornecidas todas as licenças, sem custo adicional, pelo mesmo período solicitado pela garantia e suporte deste item (com exceção do Item 04 “FIREWALL TIPO 3”);

5.3.15. Outros Requisitos

5.3.15.1. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação;

5.3.15.2. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes;

5.3.15.3. Fabricante deve comprovar participação no MAPP da Microsoft;

5.3.16. Garantia e Suporte:

5.3.16.1. Deverá ser fornecido garantia e suporte técnico, prestado diretamente pelo FABRICANTE, por 60 (sessenta) meses, contados a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos;

5.3.16.2. O serviço de suporte deve incluir atualização da solução, isto é, o fornecimento de versão ou release mais recente dos softwares e da base de conhecimento;

5.3.16.3. O serviço de suporte deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

5.3.16.4. Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de até 05 (cinco) dias úteis após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na Sede da CONTRATANTE. Esse prazo poderá ser negociado em casos excepcionais, por meio de justificativa documentada pela CONTRATADA e aceita pelo CONTRATANTE;

5.3.16.5. A reposição antecipada deve ocorrer durante o período necessário em que o equipamento da CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;

5.3.16.6. A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente da CONTRATANTE;

5.3.16.7. Para os serviços de suporte técnicos, o FABRICANTE deverá possuir Central de Atendimento disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em regime 24x7(com exceção do Item 04 “FIREWALL TIPO 3, que o regime deve ser de 8x5);

5.3.16.8. Deve possuir site na internet, com a disponibilização documentações, downloads, base de conhecimento e drivers, firmwares e todas as atualizações existentes, relativas à solução ofertada;

5.3.16.9. Devido à necessidade de atendimento de suporte da CONTRATANTE, caso o licitante não seja o mesmo fabricante da solução ofertada, este deverá enviar, juntamente com a sua proposta, declaração do fabricante da solução garantindo que prestará o serviço de suporte e garantia nas condições, localidades e atendimento nos termos deste edital ou comprovar através de PART NUMBER a totalidade do serviço contratado;

5.4. LOTE 1 - ITEM 02: FIREWALL TIPO 1 (CARACTERÍSTICAS ESPECÍFICAS)

5.4.1. Características Gerais

5.4.1.1. Compatível para montagem em rack de 19”, possuindo altura máxima de 2U, sendo que deverão ser fornecidos os respectivos kit’s de fixação;

5.4.1.2. Deve possuir no mínimo 16 (dezesseis) interfaces 10/100/1000Base-T, todas operando em modo auto-sense e em modo half/full duplex, com inversão automática de polaridade;

5.4.1.3. Deve possuir no mínimo 01 (uma) interface 10-GbE SFP+;

5.4.1.4. Possuir uma interface de rede dedicada operando em 1Gbps para o gerenciamento do produto. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

5.4.1.5. Possuir fontes de alimentação redundantes internas ao equipamento com ajuste automático de tensão 110 ou 220 volts;

5.4.1.6. O equipamento deverá ter ventiladores redundantes;

5.4.1.7. Dos 02 (dois) appliances solicitados para este item, 1 (um) deve-se ser HA;

5.4.1.8. Cada fonte de alimentação fornecida deverá acompanhar pelo menos 02 (dois) cabos de alimentação, sendo um com conector padrão NBR14136 e outro com conector padrão C14, ambos com pelo menos 1,8 metros de comprimento e em conformidade com as especificações elétricas da fonte ofertada;

5.4.2. Características de Capacidade e Performance:

5.4.2.1. A performance de Firewall SPI (Stateful Packet Inspection) deve ser de no mínimo 5 Gbps;

5.4.2.2. Deve suportar, em modo firewall, no mínimo 500.000 (quinhentos mil) de conexões concorrentes;

5.4.2.3. Deve suportar no mínimo 20.000 (vinte mil) novas conexões por segundo;

5.4.2.4. Performance de todos os serviços NGFW ativos (Firewall, IPS e Controle de Aplicativos) deverá ser de no mínimo 3 Gbps;

5.4.2.5. A performance de IPS deve ser de no mínimo 3 Gbps;

5.4.2.6. A Performance de VPN IPSEC (3DES & AES 256) deverá ser de no mínimo 2 Gbps;

5.4.2.7. Deve suportar no mínimo 500 (quinhentos) túneis VPN IPSEC do tipo site-to-site já licenciadas;

5.4.2.8. Deve suportar no mínimo 500 (quinhentos) túneis VPN IPSEC do tipo client-to-site e, caso houver licenciamento adicional para esta funcionalidade, o equipamento deve ser ofertado com no mínimo 50 (cinquenta) túneis já licenciados, suportando no futuro a utilização de mais túneis, baseado na aquisição de licenciamento adicional;

5.4.2.9. Deve suportar no mínimo 500 (quinhentas) conexões clientes do tipo SSL VPN (VPNClient) e, caso houver licenciamento adicional para esta funcionalidade, o mesmo não precisa ser ofertado;

5.5. LOTE 1 - ITEM 03: FIREWALL TIPO 2 (CARACTERÍSTICAS ESPECÍFICAS)

5.5.1. Características Gerais

5.5.1.1. Compatível para montagem em rack de 19", possuindo altura máxima de 2U, sendo que deverão ser fornecidos os respectivos kit's de fixação;

5.5.1.2. Deve possuir no mínimo 08 (oito) interfaces 10/100/1000Base-T, todas operando em modo auto-sense e em modo half/full duplex, com inversão automática de polaridade;

5.5.1.3. Deve possuir no mínimo conexão USB 3.0;

5.5.1.4. Possuir uma interface de rede dedicada operando em 1Gbps para o gerenciamento do produto. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

5.5.1.5. Possuir fonte de alimentação com ajuste automático de tensão 110 ou 220 volts;

5.5.1.6. Cada fonte de alimentação fornecida deverá acompanhar pelo menos 01 (um) cabo de alimentação, com conector padrão NBR14136;

5.5.2. Características de Capacidade e Performance:

5.5.2.1. A performance de Firewall SPI (Stateful Packet Inspection) deve ser de no mínimo 2,5 Gbps;

5.5.2.2. Deve suportar, em modo firewall, no mínimo 200.000 (duzentos mil) de conexões concorrentes;

5.5.2.3. Deve suportar no mínimo 8.500 (oito mil e quinhentos) novas conexões por segundo;

5.5.2.4. Performance de todos os serviços NGFW ativos (Firewall, IPS e Controle de Aplicativos) deverá ser de no mínimo 1 Gbps;

5.5.2.5. A performance de IPS deve ser de no mínimo 1 Gbps;

5.5.2.6. A Performance de VPN IPSEC (3DES & AES 256) deverá ser de no mínimo 1,3 Gbps;

5.5.2.7. Deve suportar no mínimo 100 (cem) túneis VPN IPSEC do tipo site-to-site já licenciadas;

5.5.2.8. Deve suportar no mínimo 200 (duzentos) túneis VPN IPSEC do tipo client-to-site e, caso houver licenciamento adicional para esta funcionalidade, o equipamento deve ser ofertado com no mínimo 5 (cinco) túneis já licenciados, suportando no futuro a utilização de mais túneis, baseado na aquisição de licenciamento adicional;

5.5.2.9. Deve suportar no mínimo 100 (cem) conexões clientes do tipo SSL VPN (VPNClient) e, caso houver licenciamento adicional para esta funcionalidade, o mesmo não precisa ser ofertado;

5.6. LOTE 1 - ITEM 04: FIREWALL TIPO 3 (CARACTERÍSTICAS ESPECÍFICAS)

5.6.1. Características Gerais

5.6.1.1. Compatível para montagem em rack de 19", possuindo altura máxima de 2U, sendo que deverão ser fornecidos os respectivos kit's de fixação;

5.6.1.2. Deve possuir no mínimo 08 (oito) interfaces 10/100/1000Base-T, todas operando em modo auto-sense e em modo half/full duplex, com inversão automática de polaridade;

5.6.1.3. Deve possuir no mínimo conexão USB 3.0;

5.6.1.4. Possuir uma interface de rede dedicada operando em 1Gbps para o gerenciamento do produto. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

5.6.1.5. Este appliance será utilizado como Spare (reserva) e, portanto, não será necessário ser ofertado licença para os módulos de proteção, exceto se o fabricante não permitir a migração das licenças que estão aplicadas em um dos appliances do mesmo modelo que estiver em produção e apresentar defeito;

5.6.1.6. Possuir fonte de alimentação com ajuste automático de tensão 110 ou 220 volts;

5.6.1.7. Cada fonte de alimentação fornecida deverá acompanhar pelo menos 01 (um) cabo de alimentação, com conector padrão NBR14136;

5.6.2. Características de Capacidade e Performance:

5.6.2.1. A performance de Firewall SPI (Stateful Packet Inspection) deve ser de no mínimo 2,5 Gbps;

5.6.2.2. Deve suportar, em modo firewall, no mínimo 200.000 (duzentos mil) de conexões concorrentes;

5.6.2.3. Deve suportar no mínimo 8.500 (oito mil e quinhentos) novas conexões por segundo;

5.6.2.4. Performance de todos os serviços NGFW ativos (Firewall, IPS e Controle de Aplicativos) deverá ser de no mínimo 1 Gbps;

5.6.2.5. A performance de IPS deve ser de no mínimo 1 Gbps;

5.6.2.6. A Performance de VPN IPSEC (3DES & AES 256) deverá ser de no mínimo 1,3 Gbps;

5.6.2.7. Deve suportar no mínimo 100 (cem) túneis VPN IPSEC do tipo site-to-site;

5.6.2.8. Deve suportar no mínimo 200 (duzentos) túneis VPN IPSEC do tipo client-to-site;

5.6.2.9. Deve suportar no mínimo 100 (cem) conexões clientes do tipo SSL VPN (VPNClient) e, caso houver licenciamento adicional para esta funcionalidade, o mesmo não precisa ser ofertado;

5.7. LOTE 1 - ITEM 05: SERVIÇOS DE INSTALAÇÃO

5.7.1. Requisitos Gerais

5.7.1.1. A CONTRATADA deverá realizar a instalação física e configuração lógica dos produtos que compõe este LOTE (NGFWs, Solução de Logs e Solução de Gerenciamento Centralizado), conforme quantitativo adquirido;

5.7.1.2. Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados;

5.7.1.3. Os serviços de implantação deverão ser executados presencialmente nas instalações da CONTRATANTE por técnico(s) da CONTRATADA capacitado(s) para tal;

5.7.1.4. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

5.7.1.5. Após e recebimento dos equipamentos e das licenças, a CONTRATANTE deverá definir, juntamente com a CONTRATADA, o cronograma de instalação e configuração dos mesmos, enviando a CONTRATADA, documento contendo informações de Data, Hora, Local, e soluções a serem instaladas;

5.7.1.6. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como fins de semana e feriados;

5.7.1.7. Deverá ser agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

5.7.1.8. Deverá ser realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

5.7.1.9. Deverá ocorrer a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, por exemplo);

5.7.1.10. Deverá ser validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

5.7.1.11. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reunião de pré-projeto, devendo a CONTRADADA sugerir as configurações de acordo com normas e boas práticas, cabendo a CONTRATANTE a aceitação ou não;

5.7.1.12. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega das soluções. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

5.7.1.13. A CONTRATADA deverá realizar a instalação física e lógica “assistida” de todos os equipamentos, componentes e softwares, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

5.7.1.14. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

5.7.1.15. Após a conclusão dos serviços de instalação, o técnico da CONTRATADA deverá realizar o monitoramento da solução por pelo menos 03 (três) dias úteis, com acompanhamento da equipe da CONTRATANTE, a fim de identificar e sanar eventuais inconsistências;

5.7.1.16. Mesmo ao final da Implantação, a CONTRATANTE poderá solicitar, dentro de um período de 30 (trinta) dias e sem qualquer ônus, apoio à CONTRATADA para sanar dúvidas em relação funcionamento da solução;

5.7.1.17. Ao término da instalação, a CONTRATADA deverá entregar Caderno de Documentação “As Built” do Projeto, no qual conste todos os detalhes da instalação, tais como:

5.7.1.17.1. Descrição dos serviços implantados;

5.7.1.17.2. Descrição de topologia lógica e de topologia física de equipamentos após a ativação dos serviços;

5.7.1.17.3. Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;
5.7.1.17.4. Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;
5.7.1.17.5. Definição de responsabilidades;
5.7.1.17.6. Recursos de alta disponibilidade;
5.7.1.17.7. Procedimentos para abertura e atendimento a chamados;
5.7.1.17.8. Procedimentos de recuperação de equipamentos;
5.7.1.17.9. Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;
5.7.1.17.10. Documentação dos processos de trabalho associados ao item;
5.7.1.17.11. Desenho dos racks onde estão instalados os equipamentos (bayface);
5.7.1.17.12. Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos);

5.7.2. Escopo dos Serviços de Implantação da Solução de Firewall:

5.7.2.1. Instalação e Configuração do Software de Gerenciamento Centralizado, quando aplicável;
5.7.2.2. Instalação das Soluções de Firewall, conforme contratado;
5.7.2.3. Configurar as Soluções de Firewall conforme segmentação de rede definida pela CONTRATANTE;
5.7.2.4. Atualização e aplicação de correções nas soluções de Firewall;
5.7.2.5. Implementação/migração de regras de Filtragem;
5.7.2.6. Implementação/migração de regras de NAT;
5.7.2.7. Implementação/migração de regras de QoS;
5.7.2.8. Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
5.7.2.9. Implementação de balanceamento e alta disponibilidade de links;
5.7.2.10. Integração com o Active Directory;
5.7.2.11. Tunning de configuração e regras de filtragem, removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados;
5.7.2.12. Testes gerais, validando o funcionamento das aplicações após a implementação dos Firewalls;

5.7.3. Local para realização dos serviços de Implantação:

5.7.3.1. A CONTRATANTE poderá contratar os serviços de Implantação para quaisquer uma de suas localidades;
5.7.3.2. As localidades para realização dos serviços são:
5.7.3.2.1. Unidade Operativa do Senac Araguaína – Gerencia da UOP. Telefone: 63 3321-5200. Endereço: Rua F, Qd AA, Lote 3, Setor George Yunes, CEP: 77.804-970, Araguaína - TO.
5.7.3.2.2. Unidade Operativa do Senac Gurupi – Gerencia da UOP. Telefone: 63 3301-4200. Endereço: Rua D, Quadra 10, Lotes 01 a 05, S/N, Bairro Engenheiro Waldir Lins (Continuação), CEP: 77.423-030, Gurupi – TO
5.7.3.2.3. Centro de Educação Profissional do Senac em Palmas – Coordenação de Compras e Licitações. Telefone: 63 3219-1627. Endereço: Quadra 201 Norte, Avenida LO-04, Conjunto 03, Lotes 03 e 04, Sala 312, CEP 77.001-132, Palmas – TO.
5.7.3.2.4. Administração Regional – Senac Tocantins. Telefone: 63 3219 1653. Endereço: Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomércio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas – TO.
5.7.3.2.5. Unidade Operativa de Idiomas – Gerência da UOP. Telefone: 63 3219 1677. Endereço: Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomércio, 2º Andar, Plano Diretor Norte, CEP: 77.001-004, Palmas – TO.

5.8. LOTE 1 - ITEM 06: SERVIÇOS DE TREINAMENTO OFICIAL (VOUCHER)

5.8.1. Características Gerais

5.8.1.1. A CONTRATADA deverá fornecer voucher para Treinamento Oficial da solução de Firewall para equipe da técnica da CONTRATANTE, conforme os conteúdos mínimos indicados a seguir, com o intuito de assegurar a transferência de conhecimento para os Administradores de Redes e Analistas de Segurança da CONTRATANTE.

5.8.1.2. O treinamento deve ser na modalidade online, ou deverá ocorrer nas instalações da CONTRATANTE, na cidade de Palmas – TO;

5.8.1.3. O treinamento deverá ser ministrado por instrutor capacitado para tal, onde a contratada deverá comprovar no momento da execução do treinamento, através das certificações do fabricante da solução, a capacitação do instrutor;

5.8.1.4. As despesas decorrentes do serviço de treinamento como: confecção do material didático, deslocamentos, hospedagem e alimentação do instrutor designado pela CONTRATADA, serão de sua própria responsabilidade;

5.8.1.5. O treinamento deverá ser ministrado no idioma português, no entanto será aceito o fornecimento de materiais no idioma inglês;

5.8.1.6. O treinamento será de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e softwares da solução ofertada, em seus aspectos mais relevantes;

5.8.1.7. Para a consecução da parte prática do treinamento, deverão ser utilizados os equipamentos ofertados, além de todos os softwares que fizerem parte da solução, antes de suas ativações efetivas, fazendo a explanação das arquiteturas das soluções e seus componentes, rotinas de administração e gerenciamento do ambiente;

5.8.1.8. A CONTRATADA deverá emitir um certificado de participação do treinamento para cada aluno, mediante presença mínima em 75% do curso, comprovada por meio da lista de presença por ele assinada diariamente;

5.8.1.9. O treinamento deverá ser concluído em até 30 (trinta) dias após a assinatura do contrato;

5.8.1.10. O treinamento deverá ser aprovado por pelo menos 70% dos participantes do treinamento. Caso o treinamento seja considerado inadequado, a CONTRATADA deverá realizar novamente o serviço, às suas expensas, após realizar os ajustes necessários no material didático ou selecionar novo instrutor. Ocorrendo 2 (duas) rejeições do treinamento, a Administração poderá rescindir o contrato por inexecução;

5.8.1.11. Ao final do treinamento, os profissionais treinados deverão estar aptos a executar as seguintes atividades:

- 5.8.1.11.1. Instalação e configuração da Solução Firewall;
- 5.8.1.11.2. Implementação de regras de Filtragem;
- 5.8.1.11.3. Implementação de regras de NAT;
- 5.8.1.11.4. Implementação de regras de QoS;
- 5.8.1.11.5. Implementação de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
- 5.8.1.11.6. Implementação de balanceamento e alta disponibilidade de links;
- 5.8.1.11.7. Integração com o Active Directory;
- 5.8.1.11.8. Monitoramento dos serviços de redes;
- 5.8.1.11.9. Filtro de informações através de relatórios;
- 5.8.1.11.10. Atualização e aplicação de correções na solução de Firewall;
- 5.8.1.11.11. Backup e Restore do Solução de Firewall;

5.8.1.12. Ao final do treinamento todos os alunos instruídos deverão receber as provas para certificação oficial do fabricante sem custo adicional ao projeto;

5.8.1.13. A carga horária total do treinamento deverá ser de no mínimo 16 (dezesseis) horas e o voucher ofertado deverá ser individual para cada participante;

5.9. LOTE 1 – ITEM 07: SERVIÇOS DE GERENCIAMENTO E SUPORTE CONTINUADO - SOLUÇÃO DE FIREWALL (HORAS)

5.9.1. Características Gerais

5.9.1.1. Será realizado como prestação de serviço, sob demanda, com banco de horas;

5.9.1.2. O saldo do banco de horas terá validade de 12 (doze) meses, sendo descontado e pago mensalmente o valor correspondente às horas usadas do banco;

5.9.1.3. O serviço poderá ser realizado remotamente (através de software próprio da CONTRATADA) ou presencialmente, conforme necessidade para a solução da requisição/incidente;

5.9.1.4. A CONTRATADA poderá disponibilizar, no ato de abertura do incidente ou requisição pela CONTRATANTE, dependendo do nível de criticidade do atendimento, que o atendimento seja feito de maneira presencial ou de maneira remota;

5.9.1.5. O atendimento deverá ser realizado por profissionais que possuam experiência comprovada para o atendimento completo das soluções. Para tal comprovação, deverá ser apresentado, no ato da assinatura do contrato, pela CONTRATADA ao menos 1 (um) profissional certificado pelo fabricante da solução proposta;

5.9.1.6. A solicitação do serviço será feita pelo CONTRATANTE, através de chamado (eletrônico ou telefônico), e-mail ou documento oficial, expedido ao prestador;

5.9.1.7. O período de abertura e resolução dos chamados será contabilizado no regime 24x7 (24 horas e 7 dias da semana);

5.9.1.8. Os prazos de atendimento deverão obedecer aos níveis de serviço conforme criticidade, descritas no item “Os tipos de criticidade e o tempo de atendimento (SLA)” mais adiante;

5.9.1.9. A CONTRATADA deverá dispor de telefone em DDD (63) ou número 0800 ou permitir ligações à cobrar para a abertura de chamados;

5.9.1.10. A CONTRATADA deverá disponibilizar e-mail para a abertura de chamados;

5.9.1.11. O acesso ao ambiente (incluindo o caso de atendimento remoto) será supervisionado por profissional da CONTRATANTE. A CONTRATADA obriga-se a respeitar as políticas de segurança e de sigilo impostas pela CONTRATANTE;

5.9.1.12. Será realizado o gerenciamento, monitoramento e suporte diário do ambiente, com desconto no banco de horas de **15h (quinze horas)** para cada mês. É necessário a apresentação de relatórios fixos mensal com no mínimo:

- 5.9.1.12.1. Número de chamados abertos e estatísticas de tipo, criticidade, tempo de resolução, entre outros filtros;
- 5.9.1.12.2. Tempo médio de atendimento de chamados;
- 5.9.1.12.3. Usuários com maior atividade permitida (pelo endereço IP/nome do usuário);
- 5.9.1.12.4. Domínios mais acessados;
- 5.9.1.12.5. Categorias de site mais acessadas;
- 5.9.1.12.6. Aplicações mais acessadas;
- 5.9.1.12.7. Categorias de aplicações mais acessadas;
- 5.9.1.12.8. Aplicações bloqueadas;
- 5.9.1.12.9. Categorias de aplicações mais bloqueadas;
- 5.9.1.12.10. Protocolos IP com maior atividade (entrada e saída);
- 5.9.1.12.11. Relatório de malwares detectados;
- 5.9.1.12.12. Relatório de tentativas de intrusão.

5.9.1.13. Os relatórios acima não serão descontados das horas disponíveis do banco de horas além do limite de 15h (quinze horas) mensais. Na data de entrega da instalação do projeto, será realizada reunião para alinhamento dos relatórios mensais fixos;

5.9.1.14. Novos relatórios poderão ser solicitados pela CONTRATANTE, sem adição de custos ou consumo de horas adicionais, desde que os dados sejam relativos ao sistema de gerenciamento de chamados ou que sejam variações dos relatórios fixos listados anteriormente;

5.9.1.15. Caso seja necessário a criação de rotina automatizada ou a criação de qualquer procedimento para a coleta de dados para a confecção de relatório fixo diverso aos já elencados, será acordado entre as partes o desconto de horas a ser realizado pelos ajustes;

5.9.1.16. As atividades que compreendem o atendimento serão:

5.9.1.16.1. Dúvidas técnicas sobre a configuração dos componentes de hardware e software que compõem o projeto, ou outras;

5.9.1.16.2. Atualizações de firmwares/microcódigos de todos os componentes de hardware e software da solução;

5.9.1.16.3. Testes de performance, segurança e disponibilidade dos serviços;

5.9.1.16.4. Inclusão/exclusão/alteração de regras, nos equipamentos Firewall, com análise crítica a fim de garantir a gestão de mudanças no ambiente da CONTRANTE;

5.9.1.16.5. Identificar brechas e vulnerabilidades na configuração de regras implantadas e propor, de forma contínua, melhorias na proteção do ambiente, sempre que identificado a necessidade;

5.9.1.16.6. Monitoramento do acesso não intrusivo de conectividade e consumo de banda do acesso, sem visibilidade dos dados trafegados pela rede;

5.9.1.16.7. Realização de backup periódico das configurações das soluções;

5.9.1.16.8. Restauração das configurações das soluções, quando houver necessidade;

5.9.1.16.9. Criar regras de QoS para controle de tráfego de aplicações, quando aplicável;

5.9.1.16.10. Realizar análise e diagnóstico do ambiente para resolução de problemas;

5.9.1.16.11. Resolução de problemas do ambiente com base nas criticidades mencionadas no acordo de nível de serviço;

5.9.1.16.12. Abrir e acompanhar os chamados de suporte junto aos fabricantes das soluções, quando for o caso;

5.9.1.17. A CONTRATADA deverá monitorar remotamente os eventos abaixo relacionados e alertar a CONTRANTE para as providências cabíveis:

5.9.1.17.1. Intrusões detectadas pelos módulos de IPS e antivírus do equipamento de Firewall UTM ofertado;

5.9.1.17.2. Indisponibilidade do cluster, quando houver, de Firewall;

5.9.1.17.3. Indisponibilidade de VPN;

5.9.1.17.4. Indisponibilidade dos links de Internet;

5.9.1.17.5. Sobrecarga de processamento;

5.9.1.18. Os tipos de criticidade e o tempo de atendimento (SLA) serão:

5.9.1.18.1. Criticidade 1 – Falha de hardware ou software que não comprometa o funcionamento do ambiente, que não gera indisponibilidade dos serviços, mas que alarma ou sinaliza falha em componentes físicos ou virtuais, falha em rotinas ou necessidades de atualizações;

5.9.1.18.2. SLA Criticidade 1 - Atendimento em até 16 horas úteis (8x5) após abertura do chamado;

5.9.1.18.3. Criticidade 2 – Falha de hardware ou software que não comprometa o funcionamento do ambiente e serviços, porém, que aciona componentes e funcionalidades de redundância, expondo o ambiente à um possível problema e parada em caso de nova falha;

5.9.1.18.4. SLA Criticidade 2 – Atendimento em até 10 horas úteis (8x5) após abertura do chamado;

5.9.1.18.5. Criticidade 3 - Falha de hardware ou software que comprometa o funcionamento do ambiente e serviços, gerando indisponibilidade completa ou parcial de qualquer serviço crítico ou que comprometa a imagem do órgão e de suas atividades e colaboradores;

5.9.1.18.6. SLA Criticidade 3 – Atendimento em até 8 horas (24x7) após abertura do chamado;

5.9.1.19. O não atendimento dos prazos do nível de serviço ensejará no desconto percentual do pagamento a ser realizado pelo chamado aberto. O desconto será executado no fim do ciclo mensal, e será calculado da seguinte forma:

$$Tempo\ excedido\ em\ horas = T.Exc\ (arendado\ para\ maior\ inteiro)$$

$$Tempo\ máximo, em\ horas, para\ atendimento\ do\ chamado\ (por\ criticidade) = SLA$$

$$\boldsymbol{Desconto} = 25\% * \left(\frac{T.Exc}{SLA}\right)$$

5.9.1.20. O desconto máximo é limitado ao valor de 100% das horas demandadas para resolução do chamado que não atendeu ao prazo do SLA;

5.9.1.21. A CONTRATANTE poderá, justificadamente, prorrogar o prazo de atendimento das solicitações e chamados, caso julgue necessário ou pertinente;

Palmas Tocantins, 12 de dezembro de 2022.

Edmilson Teles Ribeiro
Coordenação de Tecnologia da Informação
Senac Tocantins

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO II – MODELO DE CARTA DE APRESENTAÇÃO DA PROPOSTA COMERCIAL

Ao
Serviço Nacional de Aprendizagem Comercial – Adm. Reg. no Estado do Tocantins – SENAC/TO
A/C.: Presidente da Comissão de Licitação
Ref.: Concorrência nº 11/2022.

A empresa_____, inscrita no CNPJ/MF sob nº _____, propõe ao SENAC/TO o atendimento do objeto do procedimento licitatório em referência, nos seguintes termos:

1. OBJETO:

1.1 O presente instrumento tem por objeto a atualização de solução de firewall das Unidades Operativas do Senac Tocantins.

2. PREÇOS:

NOTA IMPORTANTE 01: O processo licitatório em questão **NÃO SE TRATA DE PREGÃO PRESENCIAL**, portanto, **NÃO HAVERÁ LANCES NA SESSÃO**, a licitante deverá apresentar o seu envelope com a proposta comercial com seu menor preço.

LOTE	ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	01	**Upgrade do Software de gerenciamento centralizado SonicWall GMS para SonicWall NSM** (conforme especificações dispostas no subitem 4.2 do Termo de Referência - TR) **OU SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO similar** (conforme especificações dispostas no subitem 5.2 do TR)	1	R$ 0,00	R$ 0,00
	02	**Upgrade de appliance SonicWall NSA 3650 para SonicWall NSA 2700** (conforme especificações dispostas no subitem 4.3) **OU SOLUÇÃO DE FIREWALL TIPO 01** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.4)	2	R$ 0,00	R$ 0,00
	03	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** (conforme especificações dispostas no subitem 4.4 do TR) **OU SOLUÇÃO DE FIREWALL TIPO 02** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.5 do TR)	5	R$ 0,00	R$ 0,00
	04	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** *(sem licenças de firewall),* (conforme especificações dispostas no subitem 4.5 do TR) **OU SOLUÇÃO DE FIREWALL TIPO 03** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.6 do TR)	1	R$ 0,00	R$ 0,00
	05	**Serviços de Instalação e Configuração da Solução** (conforme especificações dispostas no subitem 4.6 do TR para solução SonicWall ou 5.7 do TR para outras soluções)	1	R$ 0,00	R$ 0,00
	06	**Serviços de Treinamento Oficial (Voucher)** – (conforme especificações dispostas no subitem 4.7 do TR para solução SonicWall e 5.8 para outras soluções)	4	R$ 0,00	R$ 0,00
	07	**Serviços de Gerenciamento e Suporte Continuado - Solução de Firewall (Horas)** – (conforme especificações dispostas no subitem 4.8 do TR para solução SonicWall e 5.9 do TR para outras soluções)	360 horas	R$ 0,00	R$ 0,00
				TOTAL DO LOTE	**R$ 0,00**

VALOR TOTAL DA PROPOSTA: R$ _____ (___extenso___).

3. PRAZO DE ENTREGA (máximo de 45 dias)**:**

4. VALIDADE DA PROPOSTA (mínimo de 90 dias)**:** _____ (___extenso___) dias.

5. FORMA E CONDIÇÕES DE PAGAMENTO:
O pagamento será realizado, em conformidade com o descrito no item 12 e demais itens do Edital em referência e Anexos.
Dados bancários para depósito:
Código e nome do Banco: _____ - _____;
Código e nome da Agência: _____ - _____;
Nº da conta corrente: _____.

6. ASSINATURA DO INSTRUMENTO DE CONTRATO:

Se declarada vencedora no certame, na qualidade de representante legal da empresa, assinará o respectivo instrumento de contrato a pessoa a seguir indicada:
Sr(a): _____
Nacionalidade: _____
Estado civil: _____
Profissão: _____
Cargo: _____
RG nº: _____ UF: _____
CPF/MF nº: _____

Por fim, declaramos que:
a) Tivemos pleno acesso e tomamos conhecimento de todos os documentos que compõem o Edital de Concorrência nº 11/2022 e nossa participação no certame ratifica nossa concordância com todos os seus termos e condições.
b) Os equipamentos serão fornecidos conforme as especificações contidas no Edital em referência, ao qual esta Proposta Comercial está vinculada, e demais informações prestadas pela área técnica do SENAC/TO que se fizerem necessárias.
c) Nos preços apresentados estão incluídas todas as possíveis despesas com encargos sociais e/ou tributos porventura incidentes, fretes, seguros, taxas, seja a que título for, e quaisquer outras relacionadas com o objeto do presente procedimento licitatório.

_____, ___de _____ de 2023.

_____
(nome e assinatura do representante legal da empresa licitante)

Obs.: Este documento deverá ser impresso em papel timbrado da empresa licitante, preenchido e devidamente assinado por seu representante legal.

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO III – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (com poderes especiais)

Recomenda-se que este anexo seja apresentado separadamente dos Envelopes nº. 01 e 02 (contendo, respectivamente, os Documentos de Habilitação e a Proposta Comercial).

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

AUTORIZAÇÃO DE REPRESENTAÇÃO
(**com poderes especiais**)

A empresa _____, com sede na Rua _____, nº. _____, na cidade de _____, estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) na Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº. _____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), através da presente autoriza o(a) Sr(a). _____, residente domiciliado(a) na Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº _____-SSP/____, e inscrito(a) no CPF/MF sob nº _____, a participar da licitação instaurada pelo SENAC/TO, acima referenciada, na qualidade de preposto de nossa empresa.

Outorga-se à pessoa supramencionada amplos poderes para acordar, renunciar a recursos e prazos recursais, discordar, receber em devolução documentação pertencente à empresa, assinar e rubricar atas, contratos e demais documentos relacionados com a licitação, a fim de agir sempre em nosso nome, com todas as prerrogativas de representante oficial para esse fim específico.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: **1- Imprimir em papel timbrado.**
2- Anexar documento comprobatório da condição de representante legal da empresa (procuração ou cópia do contrato social).

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO IV – MODELO DE AUTORIZAÇÃO DE REPRESENTAÇÃO (sem poderes especiais)

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

AUTORIZAÇÃO DE REPRESENTAÇÃO
(**sem poderes especiais**)

A empresa _____, com sede na Rua _____, nº. _____, na cidade de _____, estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) na Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº. _____- SSP/_____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), através da presente autoriza o(a) Sr(a). _____, residente domiciliado(a) na Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº _____- SSP/____, e inscrito(a) no CPF/MF sob nº _____, a participar da licitação instaurada pelo SENAC/TO, acima referenciada, na qualidade de preposto de nossa empresa.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: **1- Imprimir em papel timbrado.**
2- Anexar documento comprobatório da condição de representante legal da empresa (procuração ou cópia do contrato social).

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO V – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO AO RECURSO DE HABILITAÇÃO

Recomenda-se que este anexo seja apresentado separadamente do Envelope nº 01 (contendo os Documentos de Habilitação).

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

DECLARAÇÃO DE RENÚNCIA QUANTO AO RECURSO
(REFERENTE À FASE DE JULGAMENTO DOS DOCUMENTOS DE HABILITAÇÃO)

A empresa _____, com sede à Rua _____, nº. _____, na cidade de _____, Estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) à Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº _____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), declara desistir/renunciar à sua faculdade de interposição de recurso (e do próprio prazo recursal) contra o resultado do julgamento dos Documentos de Habilitação, dando-se, desde já, por intimada desse resultado. Declara, ainda, estar ciente de que o presente documento somente terá eficácia e gerará efeitos se todas as demais licitantes que acorrerem à presente licitação entregarem, igualmente, até o final do julgamento da fase de habilitação, as respectivas Declarações de Renúncia quanto ao Recurso na licitação acima referenciada.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: **1- Imprimir em papel timbrado.**
2- Anexar documento comprobatório da condição de representante legal da empresa (procuração ou cópia do contrato social).

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO VI – MODELO DE DECLARAÇÃO DE RENÚNCIA QUANTO AO RECURSO DAS PROPOSTAS

Recomenda-se que este anexo seja apresentado separadamente do Envelope nº 02 (contendo a Proposta Comercial).

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

DECLARAÇÃO DE RENÚNCIA QUANTO AO RECURSO
(REFERENTE À FASE DE JULGAMENTO DAS PROPOSTAS COMERCIAIS).

A empresa _____, com sede à Rua _____, nº. _____, na cidade de _____, Estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) à Rua _____, nº _____, na cidade de _____, Estado _____, portador(a) da Carteira de Identidade nº _____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), declara desistir/renunciar à sua faculdade de interposição de recurso (e do próprio prazo recursal) contra o resultado do julgamento das Propostas Comerciais, dando-se, desde já, por intimada desse resultado. Declara, ainda, estar ciente de que o presente documento somente terá eficácia e gerará efeitos se todas as demais licitantes que acorrerem à presente licitação entregarem, igualmente, até o final da fase de julgamento das propostas, as respectivas Declarações de Renúncia quanto ao Recurso na licitação acima referenciada.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: **1- Imprimir em papel timbrado.**
2- Anexar documento comprobatório da condição de representante legal da empresa (procuração ou cópia do contrato social).

EDITAL DE CONCORRÊNCIA Nº 11/2022

ESCLARECIMENTO RELATIVO AOS ANEXOS V e VI

O SENAC/TO, objetivando incentivar o uso das declarações constantes dos ANEXOS V e VI do presente Instrumento Convocatório, esclarece que tais documentos somente terão eficácia ou gerarão efeitos se, e somente se, as demais licitantes desistirem, igualmente, da interposição de recursos, abrindo mão, inclusive, dos respectivos prazos recursais estabelecidos.

Dessa forma, na prática, mesmo que todas as outras licitantes as assinem e entreguem, tais declarações não põem em risco o direito de uma licitante de interpor recursos, pois bastará que apenas uma das licitantes manifeste seu desejo de recorrer para que todas as demais declarações de renúncia percam sua validade.

COMISSÃO PERMANENTE DE LICITAÇÃO

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO VII – MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE IDADE

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

DECLARAÇÃO DE QUE NÃO EMPREGA MENOR DE IDADE

A empresa _____, com sede na Rua _____, nº. _____, na cidade de _____, estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) na Rua _____, nº _____, na cidade de _____, estado _____, portador(a) da Carteira de Identidade nº. _____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), **DECLARA**, para fins de cumprimento do disposto no inciso XXXIII do Art. 7º da Constituição Federal, que não utiliza mão de obra direta ou indireta de menores de 18 (dezoito) anos para a realização de trabalhos noturnos, perigosos ou insalubres, bem como não utiliza, para qualquer trabalho, mão de obra direta ou indireta de menores de 16 (dezesseis) anos, exceto na condição de aprendiz, a partir de 14 (quatorze) anos.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: Imprimir em papel timbrado.

EDITAL DE CONCORRÊNCIA Nº 11/2022

ANEXO VIII – MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS À HABILITAÇÃO

Ao Serviço Nacional de Aprendizagem Comercial – SENAC/TO
A/C.: Presidente da Comissão Permanente de Licitação
Ref.: EDITAL SENAC/TO/CC/11/2022

DECLARAÇÃO DE INEXISTÊNCIA DE FATOS IMPEDITIVOS À HABILITAÇÃO

A empresa _____, com sede na Rua _____, nº. _____, na cidade de _____, estado _____, inscrita no CNPJ/MF sob nº _____, neste ato representada pelo(a) Sr(a). _____, cargo/função _____, residente e domiciliado(a) na Rua _____, nº _____, na cidade de _____, estado _____, portador(a) da Carteira de Identidade nº. _____, inscrito(a) no CPF/MF sob nº _____, abaixo assinado(a), **DECLARA**, para fins do disposto no EDITAL em referência, sob as penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente procedimento licitatório. Declara, também, estar ciente da obrigatoriedade de comunicar a ocorrência de qualquer evento impeditivo superveniente a apresentação dos documentos de habilitação.

_____, _____ de _____ de 20__.

_____
Representante legal da licitante
(nome e assinatura)

Obs.: Imprimir em papel timbrado.

EDITAL DE CONCORRÊNCIA N° 11/2022

ANEXO IX – MINUTA DO CONTRATO

CONTRATO N° XX/2022
CONCORRENCIA PUBLICA N° 11/2022

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA ATUALIZAÇÃO DE SOLUÇÃO DE FIREWALL QUE ENTRE SI CELEBRAM O SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL – SENAC ADMINISTRAÇÃO REGIONAL DO TOCANTINS E A EMPRESA XXXXXXXXXXXXXXXXXXXXXXXXXXXX.

O **Serviço Nacional de Aprendizagem Comercial – SENAC AR/TO,** entidade sem fins lucrativos e de direito privado, criado pelo Decreto Lei 8.621/46, de 10 de janeiro de 1.946, CNPJ sob o nº 03.711.932/0001-30, com sede na Quadra ACSUNO-10 (101 Norte), Avenida Teotônio Segurado, Lote 02, Edifício Fecomercio, 5º Andar, Plano Diretor Norte, CEP: 77.001-004, na cidade de Palmas - TO, fone: (63) 3219-1600, representado neste ato, representado neste ato, pelo Presidente do Conselho Regional Sr. Itelvino Pisoni, brasileiro, casado, empresário, portador do CI: **TAL** emitida pela SSP/XX, CPF nº **TAL** e por sua Diretora Regional, Contadora, Lunah Brito Gomes, brasileira, solteira, portadora da CI: **TAL**, emitida pela SSP/XX, CPF nº **TAL**, residentes e domiciliados em Palmas, doravante denominado CONTRATANTE e de outro lado a empresa **(razão social)**, pessoa jurídica de direito privado CNPJ: **(número),** estabelecida na **(endereço)**, na pessoa de seu representante legal, **(número)**, portador do CPF: **(número)** e RG.: **(número)**, residente e domiciliado na cidade **(nome)**, denominada CONTRATADA, observando-se as condições estabelecidas na Concorrência Pública nº. **11/2022** constantes do Processo SENAC **(número)**, homologado e adjudicado em **(data da homologação e adjudicação da Concorrência Pública)** e as disposições da **Resolução SENAC 958/2012-CN,** publicada no D.O.U., resolvem celebrar o presente Contrato, que se regerá pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 O presente Contrato tem por objeto a **atualização de solução de firewall das Unidades Operativas do Senac Tocantins.**

1.2 Os bens a serem fornecidos pela CONTRATADA ao CONTRATANTE, e as garantias a serem prestadas são aqueles descritos no ANEXO I do Edital da Concorrência Pública n. º 11/2022, ao qual o presente instrumento está vinculado.

CLÁUSULA SEGUNDA – DOS DOCUMENTOS INTEGRANTES DESTE CONTRATO

2.1 Fazem parte do presente instrumento, independentemente de transcrição, os seguintes documentos:

2.1.1. Instrumento convocatório – Edital da Concorrência Pública n. º 11/2022 e seus anexos e/ou aditamentos;
2.1.2. Proposta Comercial da CONTRATADA, datada de XX/XX/XXXX.

CLÁUSULA TERCEIRA – DOS PREÇOS

3.1 Para todos os fins que se fizerem necessários, o valor total inicial deste CONTRATO é de **R$ 0,00 (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)**, equivalente à somatória dos preços estabelecidos nesta Cláusula.

LOTE	ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	01	**Upgrade do Software de gerenciamento centralizado SonicWall GMS para SonicWall NSM** (conforme especificações dispostas no subitem 4.2 do Termo de Referência - TR) **OU SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO similar** (conforme especificações dispostas no subitem 5.2 do TR)	1	R$ 0,00	R$ 0,00
	02	**Upgrade de appliance SonicWall NSA 3650 para SonicWall NSA 270**0 (conforme especificações dispostas no subitem 4.3) **OU SOLUÇÃO DE FIREWALL TIPO 01** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.4)	2	R$ 0,00	R$ 0,00
	03	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** (conforme especificações dispostas no subitem 4.4 do TR) **OU SOLUÇÃO DE FIREWALL TIPO 02** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.5 do TR)	5	R$ 0,00	R$ 0,00
	04	**Upgrade de appliance SonicWall TZ 500 para SonicWall TZ 370** *(sem licenças de firewall),* (conforme especificações dispostas no subitem 4.5 do TR) **OU SOLUÇÃO DE FIREWALL TIPO 03** (conforme especificações dispostas nos subitens 5.1, 5.3, 5.6 do TR)	1	R$ 0,00	R$ 0,00
	05	**Serviços de Instalação e Configuração da Solução** (conforme especificações dispostas no subitem 4.6 do TR para solução SonicWall ou 5.7 do TR para outras soluções)	1	R$ 0,00	R$ 0,00
	06	**Serviços de Treinamento Oficial (Voucher)** – (conforme especificações dispostas no subitem 4.7 do TR para solução SonicWall e 5.8 para outras soluções)	4	R$ 0,00	R$ 0,00
	07	**Serviços de Gerenciamento e Suporte Continuado - Solução de Firewall (Horas)** – (conforme especificações dispostas no subitem 4.8 do TR para solução SonicWall e 5.9 do TR para outras soluções)	360 horas	R$ 0,00	R$ 0,00
				TOTAL DO LOTE	**R$ 0,00**

CLÁUSULA QUARTA – OBRIGAÇÕES DA CONTRATANTE

4.1 São obrigações do CONTRATANTE, além das demais disposições constantes neste CONTRATO e no EDITAL:

4.1.1. Definir o local em que os equipamentos deverão ser entregues;
4.1.2. Conferir os equipamentos objeto deste Edital, por ocasião da sua entrega e execução, os quais deverão ser novos, sem qualquer tipo de uso, não podendo ser ré-manufaturados, aprovando-os, desde que atendidas às especificações previstas no ANEXO I do EDITAL, em sua plenitude;
4.1.3. Rejeitar, no todo ou em parte, aqueles equipamentos que estejam porventura em desacordo com os termos, condições, e/ou especificações constantes deste CONTRATO e do EDITAL e seus Anexos;
4.1.4. Promover os pagamentos dos valores devidos por conta deste, nos prazos e condições estipulados, se atendidos em sua plenitude, os termos e condições previstos para tal, neste CONTRATO e no EDITAL e seus Anexos;
4.1.5. Proporcionar todas as facilidades para que a CONTRATADA possa desempenhar suas atividades por conta do objeto deste, em conformidade com o previsto no presente instrumento e no EDITAL.

CLÁUSULA QUINTA – OBRIGAÇÕES DA CONTRATADA

5.1 São obrigações da CONTRATADA, além das demais disposições constantes neste CONTRATO e no EDITAL;

5.1.1. Entregar os equipamentos no endereço do CONTRATANTE, conforme o previsto neste CONTRATO e no EDITAL, em prazo não superior ao máximo estipulado para tal;
5.1.2. Entregar os equipamentos totalmente montados pelo fabricante, em embalagens por ele lacradas, todos apresentando as mesmas configurações, componentes e aparência externa;
5.1.3. Responsabilizar-se totalmente pelo transporte, descarregamento e entrega dos equipamentos no local indicado pelo CONTRATANTE, inclusive em relação à mão de obra e outros equipamentos necessários para realizar tais procedimentos;
5.1.4. Fornecer equipamentos novos (primeiro uso) e em estrita conformidade com todos os termos do EDITAL, em especial com o ANEXO I – Memorial Descritivo, Especificações Técnicas e Quantidade;
5.1.5. Substituir, sem qualquer ônus para o CONTRATANTE, em até 10 (dez) dias, os equipamentos eventualmente em desacordo com as especificações do EDITAL e, consequentemente, com o constante da sua proposta, ou que, porventura, sejam entregues com defeitos e/ou imperfeições;
5.1.6. Responder, integralmente, por perdas e danos que porventura vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita, em decorrência do objeto deste;
5.1.7. Responder por quaisquer possíveis ônus decorrentes de marcas, registros e patentes relativos aos equipamentos fornecidos;
5.1.8. Garantir que cada um dos equipamentos fornecidos por conta do objeto deste atenda, de forma individual, a todos os requisitos técnicos especificados no ANEXO I do EDITAL, e seja composto de hardware, software, firmware e acessórios necessários à sua instalação, configuração e operação completa, bem como o respectivo manual de garantia;
5.1.9. Oferecer garantia do próprio fabricante e/ou fornecedor, pelo prazo mínimo de 12 (doze) meses, conforme especificado no ANEXO I do EDITAL, para todos os componentes que integram os equipamentos, incluindo reposição de peças e mão-de-obra sendo que o prazo se iniciará a contar do aceite definitivo pelo CONTRATANTE;
5.1.10. Oferecer assistência em território Brasileiro, prestada diretamente pelo fabricante ou por empresa prestadora de serviços formalmente indicada por ele;
5.1.11. Fornecer toda a documentação e manuais técnicos, completos e necessários à instalação, configuração e operação dos equipamentos, os quais deverão estar em português ou inglês (preferencialmente nesta ordem);
5.1.12. Manter, durante a vigência deste CONTRATO, todas as condições que ensejaram sua habilitação e qualificação no respectivo procedimento licitatório;
5.1.13. Permanecer devidamente atualizada e regular perante todos os órgãos públicos, privados e/ou entidade afins, bem como em relação às disposições legais vigentes;
5.1.14. Salvo disposição expressa em contrário, não poderá ceder, transferir ou, ainda, subcontratar, no todo ou parte, os direitos e obrigações decorrentes deste contrato, a quem quer que seja, bem como ceder ou onerar os créditos que eventualmente dispuser junto ao CONTRATANTE em decorrência deste, sendo ela a única e exclusiva responsável perante o CONTRATANTE pelo cumprimento, em sua plenitude, das obrigações decorrentes da contratação.

CLÁUSULA SEXTA – DO PAGAMENTO

6.1 A CONTRATADA deverá apresentar a Nota Fiscal ou Fatura corretamente preenchida; a Nota Fiscal ou Fatura que for apresentada com erro(s) será devolvida para retificação;

6.2 A empresa deverá indicar em sua Nota Fiscal ou Fatura o banco, agência e conta corrente onde será efetuado o crédito bancário referente à execução do objeto desta Licitação;

6.3 O pagamento será efetuado em moeda corrente nacional, **no prazo de até 20 (vinte) dias consecutivos**, a contar da data de entrega dos equipamentos, desde que tenham sidos aceitos pelo SENAC/TO;

6.4 O pagamento será efetuado mediante depósito bancário em conta corrente da CONTRATADA, quando mantidas as mesmas condições iniciais de habilitação neste certame;

CLÁUSULA SÉTIMA – DO PRAZO E LOCAL PARA ENTREGA DOS EQUIPAMENTOS

7.1 A CONTRATADA entregará os equipamentos em, no máximo, 45 (quarenta e cinco) dias consecutivos, contados a partir da data da assinatura deste CONTRATO.

7.2 Os equipamentos deverão ser entregues e/ou instalados, mediante agendamento prévio, na unidade do SENAC/TO, localizada no seguinte endereço:

7.2.1. **Centro de Educação Profissional de Palmas** – AANO, Avenida LO-04, Conjunto 03, Lotes 03 e 04, Palmas - TO, CEP: 77001-132 – CNPJ: 03.711.932/0006-45.

CLÁUSULA OITAVA - DA VIGÊNCIA

8.1 O presente CONTRATO entrará em vigor na data de sua assinatura e será extinto por ocasião do cumprimento, por ambas as partes, de todas as obrigações dele decorrentes, ou seja, ao final do período de garantia dos equipamentos, **em 60 (sessenta) meses**, contados após a data de finalização da instalação/implantação do equipamento com a emissão do aceite da área solicitante.

CLÁUSULA NONA - DA CESSÃO E/OU SUBCONTRATAÇÃO

9.1 Salvo disposição expressa em contrário, a CONTRATADA não poderá ceder, transferir ou, ainda, subcontratar, no todo ou parte, o objeto do presente CONTRATO, a quem quer que seja, bem como ceder ou onerar os créditos que eventualmente dispuser junto ao CONTRATANTE em decorrência deste, sendo a CONTRATADA a única e exclusiva responsável perante o CONTRATANTE pelo cumprimento, em sua plenitude, das obrigações decorrentes do objeto deste instrumento.

CLÁUSULA DÉCIMA - DA RESCISÃO

10.1 Constituem motivos para rescisão unilateral ou administrativa do contrato, por parte do SENAC/TO, os seguintes:

10.1.1. O não cumprimento ou cumprimento irregular de cláusulas contratuais, especificações e prazos;
10.1.2. A lentidão do seu cumprimento, levando o SENAC/TO a comprovar a impossibilidade da prestação do serviço, nos prazos estipulados;
10.1.3. O atraso injustificado na entrega do objeto;
10.1.4. A subcontratação total ou parcial do seu objeto, a cessão ou transferência, total ou parcial, sem prévia anuência do SENAC/TO;
10.1.5. O cometimento reiterado de faltas na sua execução, anotadas na forma prevista neste contrato;
10.1.6. A decretação de falência ou a instauração de insolvência civil;
10.1.7. A dissolução da sociedade;
10.1.8. A alteração social ou a modificação da finalidade ou da estrutura da CONTRATADA, bem como a sua associação com outrem, fusão, cisão ou incorporação, que prejudiquem ou inviabilizem a execução do contrato;
10.1.9. Razões de interesse administrativo do SENAC/TO;

10.1.10. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato.

10.2 A rescisão do contrato poderá ser amigável, por acordo entre as partes, reduzida a termo, desde que haja conveniência para o SENAC/TO, devendo ser autorizada pela Direção Regional e Presidência do SENAC/TO.

Parágrafo único: Os casos de rescisão contratual serão formalmente motivados nos autos do processo de contratação, assegurados o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA PRIMEIRA - DAS SANÇÕES ADMINISTRATIVAS

11.1 Sem prejuízo das sanções previstas na cláusula seguinte, na hipótese de rescisão administrativa do presente contrato, o SENAC/TO reserva-se o direito de reter os créditos decorrentes do contrato até o limite dos prejuízos causados ao mesmo.

11.1.1. Inexistindo pagamento devido pelo SENAC/TO, ou sendo este insuficiente, caberá à CONTRATADA efetuar o pagamento do que for devido, no prazo máximo de 15 (quinze) dias corridos, contado da data da comunicação de confirmação da multa.

11.1.2. Não se realizando o pagamento nos termos definidos nesta cláusula, far-se-á a sua cobrança judicialmente.

CLÁUSULA DÉCIMA SEGUNDA - DAS PENALIDADES

12.1 A recusa injustificada em assinar o instrumento de contrato e/ou documento equivalente, no prazo estabelecido para tal, caracterizará o descumprimento total da obrigação assumida e poderá acarretar à licitante as seguintes penalidades:

12.1.1. Perda do direito à contratação.
12.1.2. Suspensão do direito de licitar ou contratar com o SENAC por até 02 (dois) anos.

12.2 O inadimplemento total ou parcial das obrigações contratuais assumidas dará ao SENAC/TO o direito de rescindir unilateralmente o contrato, sem prejuízo de outras penalidades previstas neste Instrumento Convocatório ou no contrato ou documento equivalente, em especial:

12.2.1. Advertência por escrito.
12.2.2. Multa de 0,33% (trinta e três centésimos por cento) por dia de atraso na entrega dos equipamentos, calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, para atrasos de até 10 (dez) dias corridos em relação à data prevista para o cumprimento da obrigação em sua totalidade.
12.2.3. Multa de 10% (dez por cento), não cumulativa com a multa prevista no subitem 14.2.2 acima, calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, para atrasos acima de 10 (dez) dias corridos em relação à data prevista para o cumprimento da obrigação em sua totalidade, ou por seu não cumprimento.
12.2.4. Multa de 2% (dois por cento), calculada sobre o valor total do correspondente instrumento de contrato ou documento equivalente, por qualquer outro incidente que configure o descumprimento das obrigações contratadas, com exceção daqueles especificados nos subitens 12.2.2 e 12.2.3 acima.
12.2.5. Suspensão do direito de licitar ou contratar com o SENAC por até 02 (dois) anos.

12.3 As penalidades de cunho pecuniário eventualmente impostas à licitante eventualmente contratada por conta do objeto deste terão seus valores descontados dos possíveis créditos que esta disponha junto ao SENAC/TO, decorrentes de parcelas vencidas e ainda não pagas ou parcelas vincendas, ou ainda, recolhidos diretamente junto à área financeira deste, no prazo de até 15 (quinze) dias corridos, contados da data da sua comunicação, ou, ainda, cobrados judicialmente, quando assim se fizer necessário ou se justificar. Neste caso, as despesas processuais e os honorários advocatícios serão custeados pela licitante eventualmente contratada.

CLÁUSULA DÉCIMA TERCEIRA – DA FISCALIZAÇÃO DO CONTRATO

13.1 Da parte do SENAC/TO, a responsabilidade pela fiscalização do presente CONTRATO será da Coordenação de Saúde do CEP - Palmas, os quais administrarão, controlarão e avaliarão a execução do seu objeto em todos os seus termos.

CLÁUSULA DÉCIMA QUARTA – PROTEÇÃO DE DADOS

14.1 A CONTRATADA, por si, seus colaboradores ou prepostos, obriga-se, a atuar no presente Contrato em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física ("Titular") identificada ou identificável ("Dados Pessoais") e as determinações de órgãos reguladores/fiscalizadores sobre a matéria;

14.2 A Contratada seguirá as instruções recebidas pelo SENAC em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, devendo a Contratada garantir sua licitude e idoneidade, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis;

14.3 A Contratada deverá corrigir, completar, excluir e/ou bloquear os Dados Pessoais, caso seja solicitado pelo SENAC;

14.4 A Contratada deverá notificar o Encarregado de Proteção de Dados do SENAC sobre as reclamações e solicitações dos Titulares de Dados Pessoais originadas em virtude de Tratamento de Dados Pessoais fruto deste Contrato, bem como tratar todos os Dados Pessoais como confidenciais;

14.5 A Contratada, por seus colaboradores ou prepostos, compromete-se a tratar todos os Dados Pessoais como confidenciais, exceto se já eram de conhecimento público sem qualquer contribuição da Contratada, ainda que este Contrato venha a ser rescindido e independentemente dos motivos que derem causa ao seu término ou resolução;

14.6 A Contratada compromete-se a adotar medidas, ferramentas e tecnologias necessárias para garantir a segurança dos dados e cumprir com suas obrigações, sempre considerando o estado da técnica disponível e o nível de segurança necessário;

14.7 A Contratada deverá cumprir com os requisitos das medidas de segurança técnicas e organizacionais para garantir a confidencialidade por meio de pseudonimização ou criptografia dos Dados Pessoais, inclusive no seu armazenamento e transmissão;

14.8 A Contratada compromete-se a utilizar tecnologias visando à proteção das informações em todas as comunicações com compartilhamentos de Dados Pessoais pela Contratada ao SENAC;

14.9 A Contratada deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a

destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado por ela para o tratamento de Dados Pessoais sejam estruturados de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos em Lei e às demais normas regulamentares aplicáveis;

14.10 A Contratada deverá realizar o registro de todas as atividades realizadas em seus sistemas/ambientes ("Registros") que realizem tratamento de Dados Pessoais sob determinação do SENAC, de modo a permitir a identificação de quem as realizou. Tais Registros deverão conter, no mínimo:

13.10.1. Ação;
13.10.2. Identificação de usuários do sistema;
13.10.3. Data/hora da ação, com referência UTC (Universal Time Coordinated), sendo que os relógios de seus sistemas estão sincronizados com a hora legal brasileira e de acordo com o protocolo NTP (ntp.br) de sincronização dos relógios; e
13.10.4. A Contratada somente poderá subcontratar qualquer parte dos Serviços que envolvam o tratamento de Dados Pessoais para um ou mais terceiros ("Suboperadores") mediante consentimento prévio e por escrito do SENAC. Neste caso, a Contratada deverá celebrar um contrato escrito com o Suboperador para (i) obrigar o Suboperador às mesmas obrigações impostas por este Contrato em relação à Contratada, no que for aplicável aos Serviços subcontratados, (ii) descrever os Serviços subcontratados e (iii) descrever as medidas técnicas e organizacionais que o Suboperador deverá implementar.

14.11 A Contratada deverá monitorar, por meios adequados, sua própria conformidade e a de seus funcionários e Suboperadores com as respectivas obrigações de proteção de Dados Pessoais em relação aos Serviços e deverá fornecer ao SENAC relatórios sobre esses controles sempre que solicitado por ela;

14.12 A Contratada deverá notificar o SENAC em até 24h (vinte e quatro) horas (i) de qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (ii) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (iii) de qualquer violação de segurança na Contratada ou nos seus Suboperadores; (iv) de qualquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (v) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente;

14.13 A Contratada compromete-se a auxiliar o SENAC:

13.13.1. Com a suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados Pessoais aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e
13.13.2. No cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.

14.14 O presente Contrato não transfere a propriedade ou controle dos dados do SENAC ou dos seus clientes, inclusive Dados Pessoais, para a Contratada ("Dados"). Os Dados gerados, obtidos ou coletados a partir da prestação dos Serviços ora contratados são e continuarão de propriedade do SENAC, inclusive sobre qualquer novo elemento de Dados, produto ou subproduto que seja criado a partir do tratamento de Dados estabelecido por este Contrato;

14.15 Todo e qualquer tratamento de dados fora do Brasil, depende de autorização prévia e por escrito pelo SENAC à Contratada;

14.16 Sempre que Dados ou Registros forem solicitados pelo SENAC à Contratada, esta deverá disponibilizá-los em até 48 (quarenta e oito) horas, podendo ser em menor prazo nos casos em que a demanda judicial, a norma aplicável ou o pedido de autoridade competente assim o exija. Caso a Contratada receba diretamente alguma ordem judicial para fornecimento de quaisquer Dados, deverá comunicar ao SENAC antes de fornecê-los, se possível;

14.17 O SENAC não autoriza a usar, compartilhar ou comercializar quaisquer eventuais elementos de Dados, produtos ou subprodutos que se originem, ou sejam criados, a partir do tratamento de Dados estabelecido por este contrato;

14.18 A Contratada se compromete a devolver todos os Dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que (i) o Contrato for rescindido; ou (ii) com o término do presente Contrato. Em adição, a Contratada não deve guardar, armazenar ou reter os Dados por tempo superior ao prazo legal ou necessário para a execução do presente Contrato;

14.19 Caso os Dados da Contratada estejam contidos em um banco de Dados, além de restituir este banco de Dados de inteira propriedade do SENAC em qualquer hipótese de extinção deste instrumento, a Contratada deverá remeter em adição o dicionário de dados que permita entender a organização do banco de Dados, em até 10 (dez) dias ou em eventual prazo acordado entre as Partes;

14.20 Fica assegurado ao SENAC, nos termos da lei, o direito de regresso em face da Contratada diante de eventuais danos causados por esta em decorrência do descumprimento das obrigações aqui assumidas em relação a Proteção dos Dados;

14.21 A Contratada, sempre que tiver dúvidas ou necessidades de esclarecimentos, bem como solicitações específicas, em relação ao tratamento de seus dados pessoais, pode buscar entrar em contato com o Encarregado de Proteção de Dados Pessoais do SENAC;

14.22 A Contratada reconhece e aceita que o SENAC tem o direito de realizar auditoria, por si ou por terceiro indicado pelo SENAC, de forma presencial ou remota com a finalidade de verificar a conformidade da Contratada quanto à legislação de proteção de dados aplicável;

14.23 O SENAC terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da Contratada com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a Contratada possui perante a Lei e este Contrato.

CLÁUSULA DÉCIMA QUINTA - DISPOSIÇÕES FINAIS

15.1 As omissões deste contrato e as dúvidas oriundas de sua interpretação serão sanadas de acordo com o que dispuserem o Edital da Concorrência Pública SENAC/TO n. º 11/2022 e a proposta apresentada pela CONTRATADA, prevalecendo, em caso de conflito, as disposições do edital sobre as da proposta. Respeitadas as cláusulas contratuais, cabe ressaltar que os casos omissos serão resolvidos entre as partes, em comum acordo, conforme o Regulamento de Licitações e de Contratos do SENAC ou, ainda, pelos preceitos do direito público, aplicando-se lhes, supletivamente, os princípios da teoria geral dos Contratos e as disposições do direito privado;

15.2 Qualquer eventual necessidade de alteração das cláusulas e/ou condições ora sendo pactuadas, sempre de comum acordo entre as partes, deverá ser formalizada por meio de termo aditivo a este CONTRATO;

15.3 Este CONTRATO poderá ser aditado, nas hipóteses de supressão ou acréscimo que se fizerem necessárias em relação ao seu objeto, em até 25% (vinte e cinco por cento) do valor inicial estabelecido na Cláusula Terceira.

CLÁUSULA DÉCIMA SEXTA - DO FORO

16.1 Fica eleito o foro da Comarca de Palmas, Estado do Tocantins, como o competente para dirimir quaisquer possíveis dúvidas ou controvérsias decorrentes do presente CONTRATO, que não possam ser resolvidas de comum acordo entre partes na esfera extrajudicial, com expressa renúncia a qualquer outro, ainda que privilegiado.

16.2 E por assim estarem de pleno acordo, as partes firmam o presente CONTRATO PARTICULAR SENAC/TO/n. XX/2022 **(REF. atualização de solução de firewall das Unidades Operativas do Senac Tocantins)**, em 02 (duas) vias, de igual teor e forma, na presença das testemunhas instrumentárias, para os fins de direito.

Palmas - TO, _____ de janeiro de 2023.

Lunah Brito Gomes
Diretora Regional do SENAC/TO

Itelvino Pisoni
Presidente do SENAC/TO

.....
CONTRATADA

Testemunhas:

1) _____
Nome:
CPF/MF N°

2) _____
Nome:
CPF/MF N°