I – EDITAL SESI/CN Nº: 02/2021
II – REGÊNCIA LEGAL: REGULAMENTO DE LICITAÇÕES E CONTRATOS DO SESI
III – MODALIDADE: PREGÃO ELETRÔNICO
IV – PROCESSO PRINCIPAL Nº: CN0117/2020
V – TIPO DE LICITAÇÃO/CRITÉRIO DE JULGAMENTO: MENOR PREÇO GLOBAL POR ITEM
VI – FORMA DE EXECUÇÃO DO SERVIÇO: CONFORME ESTABELECIDO NESTE EDITAL – SESI/CN – BRASILIA/DF.

INÍCIO DO RECEBIMENTO DAS PROPOSTAS: 19 de abril de 2021.
ABERTURA DA SESSÃO DE LANCES: 30 de abril de 2021, às 09h30 (Horário de Brasília).
LOCAL DA SESSÃO: www.gov.br/compras/pt-br
CÓDIGO UASG: 389001

1. DA CONVOCAÇÃO

1.1. O Serviço Social da Indústria - Conselho Nacional – SESI/CN, com sede no Setor Bancário Norte (SBN), Quadra 01, lote 28, Bloco I, 6º e 7º andares, no Edifício Armando Monteiro Neto, Brasília - DF, CEP: 70.040-913, informa aos interessados que realizará licitação na modalidade **PREGÃO,** na forma **ELETRÔNICA SESI Nº 02/2021**, com o critério de julgamento do tipo **MENOR PREÇO,** sob a forma de execução indireta, no regime de empreitada por preço **GLOBAL POR ITEM**, às **09h30 (Horário de Brasília)**, do **dia 30 de abril de 2021**, na forma estabelecida neste Edital e seus anexos, e de acordo com o Regulamento de Licitações e Contratos do Sistema SESI, devidamente publicados no DOU de 16/09/1998, com as posteriores alterações publicadas em 26/10/2001, 11/11/2002, 24/02/2006, 11/05/2011 e 23/12/2011, bem como pelas disposições deste Edital e de seus anexos.

2. DO OBJETO

2.1. Contratação de empresa especializada para fornecimento de Solução Integrada de Serviços Gerenciados de Segurança que contemplem serviços de segurança de perímetro com fornecimento de equipamentos, administração e monitoração de segurança, resposta a incidentes de segurança e transferência de conhecimento para a equipe técnica do Conselho Nacional do SESI, conforme as especificações, quantidades e demais condições constantes deste Edital e seus Anexos.

2.2. A licitação será realizada em único item.

2.3. O critério de julgamento adotado será o menor PREÇO GLOBAL do item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

2.4. O Edital e seus Anexos encontram-se disponíveis no site do Conselho Nacional do SESI, https://conselhonacionaldosesi.org.br/transparencia/editais-e-licitacoes/, no portal de compras do Governo Federal, www.gov.br/compras/pt-br, ou pelo e-mail: comissao.licitacao@cnsesi.com.br.

2.5. Para todos os efeitos, os horários estabelecidos neste Edital, avisos e durante a Sessão Pública, obedecerão ao horário oficial de Brasília – DF

2.6. Em caso de discordância existente entre as especificações deste objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

2.7. Apesar das disposições constantes no sistema do Comprasnet, a presente licitação será regida pelo Regulamento de Licitações e Contratos do SESI.

3. DA DOTAÇÃO ORÇAMENTÁRIA

3.1. As despesas para atender a esta licitação correrão por conta dos recursos previstos no orçamento anual do SESI/CN, ficando a discriminação do código orçamentário específico vinculado ao projeto para o qual sejam demandadas as ações, podendo ser aumentado de acordo com a necessidade.

4. DO PRAZO E DO LOCAL DE EXECUÇÃO DO SERVIÇO

4.1. Do prazo para execução dos serviços: implantar todos os componentes da solução no máximo de 80 (oitenta) dias corridos, a partir da assinatura do instrumento contratual, conforme disposto no Anexo I. O prazo de garantia para todos os componentes de hardware e software, assistência técnica e serviços de sustentação serão de 12 (doze) meses, da assinatura do instrumento contratual.

4.2. Do local de execução do serviço: sede do Conselho Nacional do SESI, localizada no Setor Bancário Norte, Quadra 1, bloco I, Edifício Armando Monteiro Neto, 6º na Coordenação de Tecnologia da Informação e Comunicação.

5. DA PARTICIPAÇÃO

5.1. Somente poderão participar deste Pregão Eletrônico as empresas legalmente estabelecidas no território nacional, de ramo compatível ao objeto desta licitação, que satisfaçam as condições e as exigências do presente edital, inclusive quanto à regularidade da documentação, e que estejam devidamente cadastradas no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no sítio www.gov.br/compras/pt-br

5.1.1. As licitantes arcarão com todos os custos decorrentes da elaboração e apresentação de suas propostas.

5.2. Não será admitida, nesta licitação, a participação de empresas que:

5.2.1. Que não atendam às condições deste Edital e seu(s) anexo(s);

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

5.2.3. Estejam sob decretação de falência, concordata, recuperação judicial ou extrajudicial (conforme Lei nº 11.101/2005), dissolução ou liquidação;

5.2.4. Entidades empresariais que estejam reunidas em consórcio;

5.2.5. Estejam com o direito de licitar e/ou contratar com o SESI/CN suspenso ou que por esta entidade tenham sido declaradas inidôneas.

5.2.6. Tenham participação, a que título for, de dirigentes ou empregados do SESI/CN.

5.2.7. Que possuam Certidão Positiva de Licitantes Inidôneos conferida pelo TCU.

5.3. Estarão impedidas de participar da licitação, direta ou indiretamente:

5.3.1. Empregado, dirigente ou Conselheiro do SESI/CN.

5.3.2. Empresas que tenham entre seus dirigentes, gerentes, sócios e/ou responsáveis técnicos empregados, dirigentes, Conselheiro, membro titular ou suplente da Comissão de Licitação do SESI/CN.

5.3.3. Empresas que tenham entre seus dirigentes, gerentes, sócios e/ou responsáveis técnicos cônjuge ou parente até segundo grau de empregados, dirigentes ou Conselheiro do SESI/CN.

5.4. Como requisito para a participação neste Pregão, a licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que:

5.4.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus artigos 42 a 49.

5.4.1.1. nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

5.4.1.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

5.4.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

5.4.3. cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências deste Edital e seus Anexos;

5.4.4. não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, nem menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos, nos termos da Constituição da República Federativa do Brasil, Art.7º, Inciso XXXIII.

5.4.5. inexistam fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores.

5.4.6. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.

5.5. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

6. DO CREDENCIAMENTO

6.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão Eletrônico deverão ser cadastrados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no sítio www.gov.br/compras/pt-br até o momento anterior à abertura das Propostas/Início da sessão pública de lances.

6.2. O cadastro no SICAF deverá ser feito no portal de compras do Governo Federal, no sítio www.gov.br/compras/pt-br, por meio do certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil.

6.3. O credenciamento junto ao provedor do Sistema implica a responsabilidade legal da licitante e de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão Eletrônico.

6.4. O uso da senha de acesso da licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do Sistema ou ao SESI/CN, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

6.5. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

6.6. O SESI/CN não é unidade cadastradora do Sistema Eletrônico, devendo os licitantes interessados em participar da licitação verificar no site Comprasnet as unidades cadastradoras do sistema para entrega da documentação pertinente, bem como o apoio técnico relativo à operacionalização das funcionalidades do sistema.

7. DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

7.1. Qualquer pessoa poderá, até 2 (dois) dias úteis anteriores a data de abertura, solicitar esclarecimentos e/ou impugnar o ato convocatório deste Pregão, mediante petição, na forma eletrônica, por meio do e-mail: comissao.licitacao@cnsesi.com.br, até às 17h30, observado o horário oficial de Brasília/DF ou, na impossibilidade, protocolados no SESI/CN, situado Setor Bancário Norte (SBN), Quadra 01, lote 28, Bloco I, 6º andar, no Edifício Armando Monteiro Neto, Brasília - DF, CEP: 70.040-913, no horário de 9h às 17h30, de segunda a sexta-feira, em dias úteis.

7.2. As solicitações de esclarecimentos e/ou impugnações deverão ser enviadas em papel timbrado da licitante e devidamente assinado, e, no caso de impugnação interposta por Pessoa Jurídica, deverá ser também anexado procuração ou contrato social que assegure poderes ao signatário das peças.

7.3. Caberá à Pregoeira encaminhar a impugnação, acompanhada de parecer, à Autoridade Superior, a quem compete decidir sobre a petição no prazo de 24h (vinte e quatro horas), contados a partir do dia do seu recebimento, estendo este prazo conforme a complexidade de julgamento da impugnação.

7.4. Acolhida a petição contra o ato convocatório ou havendo necessidade de prazo maior para julgamento, nova data será designada pela Pregoeira para a realização do certame, informando aos licitantes por meio do sistema.

7.5. Os problemas técnicos no servidor ou navegador do emissor quando do envio de solicitações de esclarecimentos e/ou de impugnações serão de sua própria responsabilidade.

7.6. Os pedidos de esclarecimentos e as impugnações não suspendem os prazos previstos para realização do certame.

7.7. As respostas a solicitações de esclarecimentos e impugnações serão disponibilizadas no sistema eletrônico aos interessados.

8. DO ENVIO DA PROPOSTA DE PREÇOS

8.1. Os licitantes encaminharão, exclusivamente por meio do sistema, www.gov.br/compras/pt-br, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, a partir do dia da publicação do edital até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento.

8.2.O Envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

8.3. A apresentação da proposta implicará plena aceitação, por parte da proponente, de todas as condições estabelecidas neste Edital e seus Anexos.

8.4. A licitante será responsável por todas as transações que forem efetuadas em seu nome, no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao SESI/CN responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

8.5. Todos os custos decorrentes da elaboração e apresentação das Propostas serão de responsabilidade exclusiva da licitante, não cabendo qualquer responsabilidade ao SESI/CN, inclusive, pelas transações que forem efetuadas em seu nome no sistema eletrônico ou de eventual desconexão.

8.6. A elaboração da proposta de preços é de inteira responsabilidade do licitante, não lhe cabendo a desistência, sob pena de aplicação das sanções previstas neste Edital ou no Regulamento de Licitações e Contratos do SESI.

8.7. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

8.8. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art, 43, §1º, da LC nº 123, de 2006.

8.9. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

8.10. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

8.11. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

8.12. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

8.13. É facultado à Pregoeira realizar diligências para sanar falhas formais da proposta a exemplo de: erros numéricos, erros de cálculo, divergência entre preços unitários, subtotais e final.

8.14. Serão desclassificadas as propostas de preços que não atenderem as exigências do presente Edital e seus Anexos, quer sejam por omissão ou por apresentarem irregularidades insanáveis.

9. DA ABERTURA DA SESSÃO PÚBLICA

9.1. A partir das **09h30 do dia 30 de abril de 2021** e em conformidade com este Edital, por meio de sistema eletrônico, no site www.gov.br/compras/pt-br, será aberta a sessão pública do **Pregão Eletrônico SESI/CN Nº 02/2021**, com a divulgação pela Pregoeira das Propostas de Preços recebidas e início da etapa de lances.

9.2. Durante a sessão pública, a comunicação entre a Pregoeira e as licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

9.3. Caberá a licitante acompanhar as operações no sistema eletrônico durante o processo licitatório, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

10. DA CLASSIFICAÇÃO DAS PROPOSTAS

10.1. Os preços constantes no Termo de Referência correspondem à referência de preço máximo aceitáveis a que o SESI/CN está disposto a pagar pelo objeto da licitação.

10.2. A apresentação de proposta com valor acima do estimado pelo SESI/CN não implicará na sua desclassificação automática, sendo facultado à licitante a readequação dos valores por meio da oferta de lances sucessivos.

10.3. A Pregoeira verificará as propostas apresentadas, desclassificando aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital.

10.3.1. Também será desclassificada a proposta que identifique o licitante.

10.4. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

10.5. O Sistema ordenará, automaticamente, as propostas classificadas pela Pregoeira, sendo que somente estas participarão da fase de lance, dando início à fase competitiva.

11. DA FORMULAÇÃO DOS LANCES

11.1. Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do certame, sendo também responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

11.2. Iniciada a sessão de lances, as licitantes com propostas aceitas poderão, durante o horário fixado para o recebimento de lances, oferecer sucessivos lances, exclusivamente por meio do sistema eletrônico, com valores inferiores ao último por eles ofertados e registrados no sistema eletrônico, observadas as regras de aceitação estabelecidas neste Edital.

11.3. Os lances apresentados e levados em consideração, para efeito de julgamento, serão de exclusiva responsabilidade da licitante, não lhe cabendo o direito de pleitear qualquer alteração.

11.4. Em caso de falha no sistema, os lances em desacordo com os subitens anteriores deverão ser desconsiderados pelo pregoeiro, devendo a ocorrência ser comunicada imediatamente à Secretaria de Gestão do Ministério da Economia.

11.4.1. Na hipótese do subitem anterior, a ocorrência será registrada em campo próprio do sistema.

11.5. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

11.6. Durante o transcurso da sessão pública deste Pregão, as licitantes serão informadas, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes, vedada à identificação do detentor do lance.

11.7. No caso de desconexão com a Pregoeira no decorrer da sessão de lances do pregão, o sistema eletrônico poderá permanecer acessível às licitantes para a oferta dos lances.

11.7.1. A Pregoeira, quando possível, dará continuidade a sua atuação no certame, sem prejuízo dos atos realizados.

11.7.2. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão de lances do pregão será suspensa e terá reinício somente após comunicação expressa da Pregoeira aos participantes, no endereço eletrônico utilizado para divulgação.

11.8. Neste Pregão o modo de disputa adotado é o aberto, assim definido no inciso I art. 31º do Decreto n.º 10.024/2019.

11.8.1. O intervalo de diferença entre os lances deverá ser de, no mínimo, R$ 100,00 (cem reais), tanto em relação aos lances intermediários, quanto em relação do lance que cobrir a melhor oferta.

11.8.2. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3)

segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

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

11.8.4. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

11.8.5. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

11.8.6. Encerrada a fase competitiva sem que haja prorrogação automática pelo sistema, poderá o pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

11.8.7. Caso a licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

11.9. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

11.10. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

11.11. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

11.12. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

11.13. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

11.14. Os documentos a serem apresentados para cumprimento das exigências são os relacionados no Item 14 deste Edital.

12. DO JULGAMENTO DAS PROPOSTAS DE PREÇOS

12.1. O julgamento da proposta será pelo **MENOR PREÇO GLOBAL POR ITEM**.

12.2. Encerrada a etapa de lances a Pregoeira examinará a proposta classificada em 1º (primeiro) lugar quanto ao preço, bem como quanto ao cumprimento das especificações do objeto.

12.3. Se a proposta de menor preço não for aceitável ou se a licitante desatender as exigências da habilitação, a Pregoeira examinará a proposta subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao Edital.

13. DA NEGOCIAÇÃO

13.1. Após o encerramento da etapa de lances, a Pregoeira solicitará contraproposta diretamente à licitante que tenha apresentado o lance mais vantajoso, para que seja obtida melhor proposta, observando o critério de julgamento e o valor estimado para a contratação, não se admitindo negociar condições diferentes daquelas previstas no Edital.

13.2. A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelas demais licitantes.

14. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

14.1. A licitante classificada em 1º (primeiro) deverá enviar os documentos exigidos para habilitação, conforme item 14 deste Edital e a Proposta de Preços readequada ao último lance, por meio da funcionalidade "Enviar Anexo" do sistema eletrônico, no prazo de 02 (duas) horas, contado da convocação efetuada pela Pregoeira, sob pena de não aceitação da proposta.

14.2. Caso a licitante convocada enfrente dificuldades em atender a convocação, deverá informar, dentro do prazo previsto no item 14.1, deste edital, quando, a critério da Pregoeira, ser-lhe-á concedido um prazo adicional.

14.3. A Pregoeira poderá fixar prazo para o reenvio de anexo, quando da necessidade de envio de planilha de composição de preços, tenha sido o preço total ofertado aceitável, mas

os preços unitários que o compõem necessitem de ajustes aos valores estimados pelo SESI/CN.

14.4. Excepcionalmente, a Pregoeira poderá disponibilizar o e-mail institucional comissao.licitacao@cnsesi.com.br, caso a licitante tenha dificuldades em anexá-los ao sistema ou este não comporte o tamanho dos arquivos.

14.5. As demais licitantes participantes da sessão poderão solicitar à Pregoeira vistas dos arquivos enviados nos termos do subitem anterior, somente pelo e-mail institucional comissao.licitacao@cnsesi.com.br, no prazo máximo de 20 (vinte) minutos, após encerrado o prazo de envio da documentação.

14.6. Encerrado o prazo do subitem anterior, as vistas dos autos serão franqueadas aos interessados no endereço e horário estabelecidos neste Edital.

14.7. A Proposta de Preços a ser encaminhada em conformidade com o Anexo II deste Edital deverá conter e assegurar as seguintes informações:

14.7.1. Preço unitário e total para cada um dos itens nela constantes, em Real (R$), em algarismos arábicos em até 2 (duas) casas decimais após a vírgula, fixos e irreajustáveis durante o prazo de validade da proposta, contados a partir da abertura da sessão de lances do pregão, bem como o valor global da proposta expresso em algarismo e por extenso, não podendo nenhum dos valores unitários e totais serem superiores aos valores estimados neste Edital.

14.7.2. Declarar, expressamente, estarem previstos nos preços ofertados todos os custos diretos e indiretos pertinentes à formação dos preços do objeto, incluindo todas as despesas com tributos, fretes e entregas, seguros, taxas e demais encargos, não sendo lícita a cobrança posterior de qualquer ônus, ficando a licitante obrigada a executar o objeto pelo valor resultante de sua Proposta de Preços. Na falta de tal declaração, serão consideradas inclusas nos preços todas e quaisquer despesas vinculadas ao objeto desta licitação.

14.7.3. Garantir a qualidade da prestação de serviços, obrigando-se a corrigir, imediatamente, todos aqueles que estiverem fora do padrão estabelecido neste Edital, sem quaisquer ônus para o SESI/CN, até o efetivo atendimento das referidas propostas.

14.7.4. O número desta licitação, razão social da licitante, número de CNPJ, telefone, e-mail, se houver, e o respectivo endereço com CEP, dados bancários para efeito de pagamento (nome do banco, o código da agência e o número da conta corrente de titularidade da licitante em conformidade com o CNPJ da Proposta de Preços, bem como os dados do responsável pela assinatura do Instrumento Contratual/Contrato (nome completo, nº do documento de identidade, nº do CPF, estado civil, nacionalidade, endereço completo, profissão, cargo que exerce na empresa e e-mail).

14.7.5. O prazo de validade da proposta não inferior a **60 (sessenta) dias corridos**, contados da data da abertura da sessão de lances.

14.7.6. Descrição detalhada do objeto da licitação, em conformidade com as especificações e condições estabelecidas neste Edital e seus Anexos.

14.8. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para a língua portuguesa, efetuada por tradutor juramentado e devidamente consularizados e registrados no Cartório de Títulos e Documentos, exceto para os previstos no subitem 14.11., no que couber.

14.9. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados no Cartório de Títulos e Documentos, exceto para os previstos no subitem 14.11., no que couber.

14.10. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz.

14.11. **Dentre os documentos passíveis de solicitação pela Pregoeira, destacam-se os que contenham as características do material ofertado, tais como catálogos, folhetos, manuais ou prospectos, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pela Pregoeira, sem prejuízo do seu posterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.**

14.12. A licitante que abandonar o certame, deixando de enviar a documentação exigida, será desclassificada e sujeitar-se-á às sanções previstas neste Edital.

14.13. Os documentos remetidos por meio da opção “Enviar Anexo” do sistema eletrônico poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pela Pregoeira.

14.14. Os originais ou cópias autenticadas dos documentos deverão ser encaminhados à Coordenação de Licitações, Contratos e Suprimentos, endereço: Setor Bancário Norte (SBN), Quadra 01, lote 28, Bloco I, 6º andar, no Edifício Armando Monteiro Neto, Brasília - DF, CEP: 70.040-913.

14.15. Os documentos emitidos por cartório *on line* poderão ser apresentados, desde que acompanhados de seus respectivos certificados digitais, para conferência da Pregoeira.

14.16. O prazo estabelecido pela Pregoeira poderá ser prorrogado por solicitação escrita e justificada da licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pela Pregoeira.

14.17. Será desclassificada a proposta ou o lance vencedor com valor superior ao preço estimado ou que apresente preço manifestamente inexequível, cabendo à Pregoeira estabelecer prazo para que a licitante demonstre a exequibilidade de seu preço.

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

14.19. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da própria licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

14.20. Se a proposta ou lance vencedor for desclassificado, a Pregoeira examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

14.21. Nas hipóteses em que a Pregoeira não aceitar a proposta motivadamente e passar à subsequente, poderá negociar com a licitante para que seja obtido preço melhor.

14.22. Havendo necessidade, a Pregoeira suspenderá a sessão, informando no *"chat"* a nova data e horário para sua continuidade.

14.23. Constatado o atendimento das exigências fixadas no Edital e declarada a licitante vencedora, a Pregoeira consignará esta decisão em ata própria, que será disponibilizada no sistema eletrônico, encaminhando-se o processo à autoridade competente para homologação e adjudicação.

14.24. No valor global deverão estar inclusos todos os tributos, taxas, impostos, encargos sociais, seguros, despesas com transportes, bem como todas as obrigações trabalhistas e previdenciárias decorrentes da prestação dos serviços.

15. DOS DOCUMENTOS DE HABILITAÇÃO

15.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

15.1.1. SICAF;

15.1.2. Consulta consolidada de Pessoa Jurídica do Tribunal de Contas da União (http://certidoes-apf.apps.tcu.gov.br/);

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

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

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

15.1.3.1.2. O licitante será convocado para manifestação previamente à sua desclassificação.

15.1.4. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

15.1.5. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

15.2. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 02 (duas) horas, sob pena de inabilitação.

15.3. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

15.4. Os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

15.5. Habilitação Jurídica:

15.5.1. Registro Comercial, no caso de empresa individual, acompanhado da cédula de identidade do proprietário.

15.5.2. Ato Constitutivo, Estatuto ou Contrato Social em vigor com todas as suas respectivas alterações ou Contrato Social consolidado, devidamente registrado, em se

tratando de sociedades comerciais. No caso de sociedade por ações e/ou cooperativas, deverá ser apresentado, ainda, documento de eleição de seus administradores.

15.5.3. Inscrição do Ato Constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.

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

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

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

15.5.7. inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência.

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

15.6. Regularidade Fiscal:

15.6.1. Prova de Inscrição no Cadastro Nacional das Pessoas Jurídicas – CNPJ.

15.6.2. Prova de Inscrição no Cadastro de Contribuintes Estadual e municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

15.6.3. Prova de Regularidade junto ao Fundo de Garantia por Tempo de Serviço – CR/FGTS, emitido pela Caixa Econômica Federal.

15.6.4. Prova de Regularidade para com a Fazenda Federal, Estadual e Municipal, se houver, do domicílio ou sede da licitante, mediante apresentação de:

a) Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas

administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

b) Prova de Regularidade junto à Secretaria da Fazenda e Planejamento do Governo do Distrito Federal (para as empresas sediadas em Brasília).

c) Prova de Regularidade para com as Fazendas Estadual e Municipal (para as empresas sediadas em outras localidades).

15.7. Regularidade Trabalhista:

15.7.1. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT, conforme Lei Federal nº 12440/2011, dentro do prazo de validade.

15.8. Qualificação Econômico-Financeira:

15.8.1. Certidão negativa de falência, concordata ou recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica, dentro do prazo de validade. Nos casos em que não houver validade na própria certidão, esta deverá ter sido emitida há, no máximo, 3 (três) meses.

15.8.2. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta.

15.8.2.1. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

15.8.2.2. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

15.8.3. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

15.8.4. As empresas, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente.

15.9. Qualificação Técnica:

15.9.1. As Licitantes deverão comprovar as exigências mínimas descritas abaixo:

15.9.1.1. Comprovação de capacidade técnica, mediante apresentação de, pelo menos, 1 (um) atestado, de bom desempenho anterior, relativo à prestação de serviço de SOC de mesma natureza da presente licitação, expedido por pessoa jurídica de direito público ou privado que comprove(m) aptidão para o desempenho do serviço licitado.

15.9.1.2. Comprovação de capacidade técnica, mediante apresentação de, pelo menos, 1 (um) atestado, bom desempenho anterior, relativo à solução de Next Generation Firewall de mesma natureza da presente licitação, expedido por pessoa jurídica de direito público ou privado que comprove(m) aptidão para o desempenho do serviço licitado.

15.9.2. A Licitante deverá comprovar ainda:

15.9.2.1. Que possui, na data prevista para a entrega da proposta, ou possuirá, na data de início da prestação dos serviços, recursos operacionais e profissional(is) que detenham as certificações do fabricante da solução ofertada com comprovada regularidade para desempenho de atividades pertinentes e compatíveis com o objeto do Termo de Referência. A comprovação deverá ser por meio de Declaração firmada pelo representante legal da licitante.

15.9.2.1.1. No que concerne aos profissionais, deverão ser ao menos 02 (dois) profissionais empregados e qualificados de acordo com as certificações das soluções de perímetro empregadas na prestação dos serviços;
15.9.2.1.2. Não serão aceitas certificações de vendas, nem parcerias;
15.9.2.1.3. O SOC deverá contar com profissionais capacitados para a realização das atividades de monitoramento de segurança, contendo, no

mínimo, um profissional com os certificados válidos para, pelo menos, duas das competências abaixo:

15.9.2.1.3.1. ISO/IEC 27001, ISO/IEC 27002 ou similar;

15.9.2.1.3.2. Operação e administração da Solução de Prevenção de Ameaças de próxima geração da solução ofertada com o nível de engenheiro/administrador;

15.9.2.1.3.3. Resposta a Incidentes de Segurança;

15.9.2.1.4. O(s) Profissional(is) deverá(ão) pertencer ao quadro da Licitante, entendendo-se como tal, para fins do Termo de Referência, o sócio que comprove seu vínculo por intermédio de Contrato/Estatuto Social; o Administrador ou o Diretor; o empregado devidamente registrado em Carteira de Trabalho e Previdência Social ou ainda a comprovação da disponibilidade do profissional mediante contrato de prestação de serviços, sem vínculo trabalhista e regido pela legislação civil.

15.10. Outros documentos:

15.10.1. Declaração de que não emprega menor e Declaração de inexistência de fato superveniente impeditivo da habilitação.

15.11. A habilitação das licitantes poderá ser consultada por meio do SICAF (habilitação parcial) e dos documentos de habilitação especificados neste Edital.

15.12. As licitantes que não atenderem às exigências de habilitação parcial no SICAF deverão apresentar documentos que supram tais exigências, na forma da lei vigente.

15.13. Caso a licitante esteja com algum documento ou informação vencido ou não atualizado no SICAF, ser-lhe-á assegurado o direito de encaminhar, na própria sessão, a documentação atualizada.

15.14. Os documentos mencionados acima poderão ser apresentados em cópia simples, acompanhado(s) do original para autenticação pela Pregoeira ou por qualquer processo de cópia devidamente autenticada por tabelião de notas (Cartório) ou impressos por meio de pesquisa feita nos sítios eletrônicos dos órgãos oficiais emitentes dos referidos documentos, os quais deverão estar em perfeitas condições de legibilidade e entendimento.

15.15. Os documentos deverão ser apresentados em envelope fechado de forma indevassável e rubricados em suas partes coladas com a seguinte inscrição - **Pregão Eletrônico SESI/CN Nº 02/2021.**

15.16. Não serão aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos requeridos no presente Edital e seus Anexos.

15.17. No caso de documentos extraídos da internet, será facultado à Pregoeira realizar pesquisa para efeito de confirmação da veracidade ou validade desses.

15.18. Os documentos de habilitação deverão ser encaminhados, concomitantemente, com a proposta, exclusivamente por meio do sistema eletrônico, até a data e horário estabelecidos neste Edital.

15.19. As licitantes que não atenderem às exigências de habilitação parcial no SICAF deverão apresentar documentos que supram tais exigências.

15.20. Sob pena de inabilitação, os documentos de habilitação deverão estar em nome da licitante e conter o mesmo número do CNPJ, que deverá corresponder ao CNPJ constante da proposta da licitante. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz; e se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

15.21. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para a língua portuguesa, efetuada por Tradutor Juramentado, e também devidamente consularizados; ou registrados no Cartório de Títulos e Documentos.

15.22. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados no Cartório de Títulos e Documentos.

15.23. É facultado à Pregoeira realizar diligências para sanar falhas formais na documentação de habilitação.

15.24. No julgamento da habilitação e das propostas, a Pregoeira poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, desde que devidamente justificado.

15.25. A Pregoeira poderá suprir a eventual omissão ou falha de documentos de regularidade fiscal, mediante consulta via internet em sites oficiais que emitam certidões *on line*, registrando em ata a sua ocorrência, reconhecendo-lhes os efeitos para fins de habilitação.

15.26. As diligências mencionadas no subitem 15.23 ficarão prejudicadas caso o acesso via internet esteja indisponível, por qualquer que seja a razão, ou as informações contidas nos referidos sites não sejam suficientes para atestar a regularidade fiscal da licitante, fato que ensejará a inabilitação da empresa.

15.27. Serão inabilitadas a(s) empresa(s) que não atender(em) ao Item 15 deste Edital.

16. DOS RECURSOS ADMINISTRATIVOS

16.1. O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal e trabalhista de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

16.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

16.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

16.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

16.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

16.3. A falta de manifestação imediata e motivada da licitante importará a decadência do direito de recurso e adjudicação do objeto pela Pregoeira ao vencedor.

16.4. A decisão da Pregoeira sobre o recurso deverá ser motivada e submetida à apreciação da Autoridade Superior a quem compete decidir sob a petição.

16.5. O recurso contra decisão da Pregoeira terá efeito suspensivo.

16.6. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto e homologará o procedimento licitatório.

16.7. Os recursos deverão ser interpostos exclusivamente por meio do site www.gov.br/compras/pt-br

16.8. Não serão conhecidos os recursos interpostos após o referenciado prazo, bem como os que forem enviados por fax ou e-mail.

16.9. Os autos do processo permanecerão com vista franqueada aos interessados, na Coordenação de Licitações, Contratos e Suprimentos, endereço: Setor Bancário Norte (SBN),

Quadra 01, lote 28, Bloco I, 6º andar, no Edifício Armando Monteiro Neto, Brasília - DF, CEP: 70.040-913.

16.10. Caso a licitante classificada em primeiro lugar seja desclassificada, depois de julgados os recursos interpostos e até a homologação/adjudicação do processo licitatório, será procedida a chamada das licitantes remanescentes, na ordem de classificação, para que a segunda classificada, que preencha as condições de habilitação, seja declarada vencedora, nas condições de sua Proposta de Preços.

17. DA REABERTURA DA SESSÃO PÚBLICA

17.1. A sessão pública poderá ser reaberta:

17.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

17.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

17.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

17.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

17.2.2. A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

18. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

18.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

18.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

19. DA GARANTIA DE EXECUÇÃO

19.1. A licitante vencedora deverá apresentar ao Contratante, no prazo máximo de 15 (quinze) dias úteis, contados da data de assinatura do contrato, comprovante de prestação de garantia prévia correspondente ao percentual de 5% (cinco por cento) do valor global do contrato, podendo optar por uma das seguintes modalidades:

a) Caução em dinheiro;
b) Seguro garantia;
c) Fiança bancária.

19.1.1. Caso não haja, no prazo acima, possibilidade da apresentação da comprovação exigida no subitem 19.1, a Licitante deverá apresentar protocolo de solicitação.

19.1.2. No caso de a Contratada optar pelo seguro-garantia, poderá decidir-se por uma das seguintes alternativas:

a) Apresentar seguro-garantia para os riscos elencados no subitem 19.1.3, correspondente a 5% (cinco por cento) do valor global atualizado do contrato, na modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviço" com cláusula específica indicando a cobertura adicional de obrigações previdenciárias e/ou trabalhistas não honradas pela Contratada; ou
b) Apresentar seguro-garantia, modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviços" para cobertura constante nas alíneas "a" a "c" do subitem 19.1.3, complementada com a garantia adicional da modalidade "Seguro-Garantia de Ações Trabalhistas e Previdenciárias" para a alínea "d" do subitem 19.1.3, correspondente a 2% (dois por cento) e 3% (três por cento), respectivamente, do valor global atualizado do contrato.

19.1.3. A garantia, em qualquer das modalidades escolhidas, visa assegurar o pagamento de:

a) Eventual prejuízo decorrente do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações assumidas;
b) Eventuais prejuízos causados ao SESI – CN, ou terceiros, decorrentes de culpa ou dolo durante a execução do contrato;
c) Eventuais multas aplicadas pelo SESI-CN à Contratada; e
d) Obrigações e encargos trabalhistas, fiscais ou previdenciários de qualquer natureza, não honradas pela Contratada.

19.2. No caso de escolha da modalidade seguro-garantia, em seus termos deverá constar, expressamente, as previsões contidas nas alíneas "a" a "d" do subitem 19.1.3.

19.3. O descumprimento do prazo estabelecido no subitem 19.1 acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 10% (dez por cento).

19.4. O atraso superior a 15 (quinze) dias no cumprimento do estabelecido no subitem 19.1 poderá ensejar a rescisão do contrato por inadimplemento, sujeitando-se a Contratada às sanções estabelecidas no Regulamento de Licitações e Contratos do SESI.

19.5. A garantia emitida deverá conter, expressamente, declaração de que o responsável pela garantia possui plena ciência dos termos e condições deste instrumento convocatório.

19.6. A garantia será considerada extinta:

a) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do SESI-CN de que a Contratada cumpriu todas as cláusulas do contrato;
b) Ao final da vigência do Contrato.

19.7. A garantia deixará de ser executada nas seguintes hipóteses:

a) Caso fortuito ou força maior;
b) Alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;
c) Descumprimento das obrigações, pela Contratada, em decorrência de atos ou fatos praticados pelo SESI – CN;
d) Atos ilícitos dolosos praticados por colaboradores do SESI – CN.

19.8. Caberá ao SESI – CN apurar as isenções de responsabilidade previstas no subitem 19.7.

19.9. Não serão aceitas garantias que não as previstas neste instrumento convocatório.

19.10. Havendo a utilização da garantia para pagamento de multa que tenha sido aplicada à Contratada, esta deverá proceder à respectiva reposição no prazo de 05 (cinco) dias úteis contados da data em que for notificada da imposição da sanção.

19.11. A garantia será extinta com a emissão da DECLARAÇÃO de que a Contratada executou integralmente o objeto contratado, servindo para fins de autorização e levantamento da caução em dinheiro e extinção da garantia.

19.12. A DECLARAÇÃO de que trata o subitem anterior será emitida após o decurso do prazo de 120 (cento e vinte) dias da emissão do Termo de Encerramento de Contrato–TEC, desde que comprovado o pagamento de todas as verbas trabalhistas e previdenciárias decorrentes da contratação.

19.13. A licitante vencedora manterá a garantia de execução do contrato durante todo o prazo contratual, prorrogando-a, complementando-a ou substituindo-a, sempre com antecedência de 30 (trinta) dias à sua expiração.

19.14. A garantia deverá ser ajustada sempre que ocorrer o reajuste de preços ou eventuais diminuições de seu valor pela utilização nos casos previstos no contrato.

20. DO CONTRATO DE PRESTAÇÃO DE SERVIÇOS

20.1. Independentemente de sua transcrição, para todos os efeitos legais, farão parte do Contrato que vier a ser assinado e retirado, todas as condições estabelecidas no presente Edital e seus Anexos, na Proposta de Preços e na Documentação de Habilitação da licitante vencedora.

20.2. A licitante vencedora deverá comparecer ao SESI/CN, no prazo máximo de 5 (cinco) dias úteis, contados de sua convocação, para assinatura do Contrato, conforme modelo constante, no Anexo III.

20.3. A empresa vencedora fica obrigada a aceitar, nas mesmas condições pactuadas, os acréscimos ou decréscimos que se fizerem necessários, até 25% (vinte e cinco por cento) do valor inicial do Contrato atualizado, conforme Artigo 30 do Regulamento de Licitações e Contratos do SESI.

20.4. A vigência do Contrato de Prestação de Serviços será pelo período de 12 (doze) meses, a contar da data da assinatura, admitida a sua prorrogação, condicionada à prévia e expressa anuência das partes, formalizada mediante termo aditivo, até o limite de 60 (sessenta) meses previsto no parágrafo único do art. 26 do Regulamento de Licitações e Contratos do SESI.

21. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

21.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

22. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

22.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

23. DO PAGAMENTO

23.1. A nota fiscal/fatura, contendo o detalhamento dos serviços executados, deverá ser entregue ao Conselho Nacional do SESI, após o recebimento do serviço pelo contratante.

23.1.1. A empresa Contratada deverá apresentar nota fiscal, acompanhada da seguinte documentação: CNPJ; Prova de Inscrição no Cadastro de Contribuintes Estadual e Municipal – compatível com o objeto social; CR/FGTS; CERTIDÃO DE QUITAÇÃO DE TRIBUTOS E CONTRIBUIÇÕES FEDERAIS, INCLUINDO AS CONTRIBUIÇÕES SOCIAIS; CERTIDÃO DE REGULARIDADE DO GDF, para as empresas sediadas em Brasília; e, CERTIDÃO DE REGULARIDADE ESTADUAL E MUNICIPAL, para as empresas sediadas em outras localidades deste Edital, para liquidação e pagamento da despesa contraída pela entidade que compõem o SESI.

23.2. O pagamento deverá ser realizado em até 30 (trinta) dias, contados da medição mensal dos serviços, mediante a apresentação da Nota Fiscal/Fatura devidamente aprovada pelo Gestor do Contrato.

23.2.1. O início do pagamento previsto no subitem anterior se dará após a implementação e o pleno funcionamento da solução de SOC.

23.3. O pagamento será efetuado em até 10 (dez) dias após o recebimento da Nota Fiscal, contendo o "atesto" pelo recebimento dos serviços pelo Fiscal do contrato.

23.4. Havendo erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o Conselho Nacional do SESI.

23.5. O pagamento será creditado em favor da Contratada por meio de ordem de pagamento bancária, devendo, para isto, ficar explicitado o nome, número da agência e o número da conta corrente.

23.6. A empresa Contratada estará sujeita às retenções tributárias legais, devendo ser informado no corpo da Nota Fiscal as deduções às quais ela se adequa.

23.7. A Contratada optante pelo SIMPLES NACIONAL deverá enviar junto com a nota fiscal, a declaração de optante pelo SIMPLES NACIONAL com indicação da Lei regulamentadora.

23.8. O preenchimento da nota fiscal deverá ser conforme orientação da fiscalização, devendo a mesma conter também as informações dos tributos a serem descontados, tais como: INSS, IRPJ, CSSLL, CONFINS, PIS e ISS, quando houver.

23.9. A Nota Fiscal/Fatura, para liquidação e pagamento dos materiais e ferramentas, deverá estar obrigatoriamente atestada pela área demandante, bem como acompanhada da documentação exigida, dentro do prazo de validade.

23.10. Em hipótese alguma será efetuado pagamento por meio de boleto bancário.

23.11. Para liquidação dos valores relativos à Prestação de Serviços objeto deste Edital, o SESI/CN assegura-se o direito:

23.11.1. Recusar o pagamento caso a Prestação de Serviços do objeto não seja realizado de acordo com o proposto, aceito e pactuado.

23.11.2. Deduzir do montante a pagar as indenizações devidas pela empresa Contratada em razão da inadimplência nos termos do Contrato que vier a ser firmado.

23.11.3. Devolver à Contratada as Notas Fiscais não aprovadas para as devidas correções, acompanhadas dos motivos de sua rejeição, recontando-se para pagamento o prazo 10 (dez) dias após o recebimento da Nota Fiscal, a partir da sua reapresentação,

sem qualquer tipo de correção de seu valor, sendo automaticamente alteradas as datas de vencimento, não respondendo os proponentes do SESI/CN por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

24. DAS SANÇÕES ADMINISTRATIVAS

24.1. Comete infração administrativa, o licitante/adjudicatário que:

24.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

24.1.2. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

24.1.3. apresentar documentação falsa;

24.1.4. fraudar na execução do contrato;

24.1.5. deixar de entregar os documentos exigidos no certame;

24.1.6. ensejar o retardamento da execução do objeto;

24.1.7. não mantiver a proposta;

24.1.8. cometer fraude fiscal;

24.1.9. comportar-se de modo inidôneo;

24.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

24.3. A Contratada que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

24.3.1. Advertência por escrito.

24.3.2. Será aplicada multa pelo descumprimento dos prazos relacionados aos NÍVEIS DE ACORDO DE SERVIÇO do Termo de Referência, causado pela CONTRATADA. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

24.3.2.1. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

24.3.2.1.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,1% (um décimo por cento) ao dia do valor total do respectivo Contrato;

24.3.2.1.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea anterior será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total do respectivo Pedido de Compras / Contrato.

24.3.3. Será aplicada multa pelo atraso, causado pela CONTRATADA, no fornecimento das informações sobre os canais de atendimento. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

24.3.3.1. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

24.3.3.1.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,05% (cinco centésimos por cento) ao dia do valor total do respectivo Pedido de Compras / Contrato;

24.3.3.1.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea anterior será substituída por multa de 0,1% (um décimo por cento) ao dia, até o limite máximo de 2% (dois por cento) do valor total do respectivo Pedido de Compras / Contrato.

24.3.4. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 0,1% (um décimo por cento) à hora, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela CONTRATADA, no cumprimento dos prazos para solução das ocorrências, causado pela CONTRATADA, para cada chamado registrado pela CONTRATANTE. O descumprimento de mais de um prazo para um mesmo chamado implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

24.3.5. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela CONTRATADA, no fornecimento da solução definitiva para as ocorrências de software. O descumprimento do prazo de cada chamado registrado pela CONTRATANTE implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

24.3.6. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de até 5% (cinco por cento), pelo atraso, causado pela CONTRATADA, no fornecimento de qualquer um dos relatórios solicitados, do Termo de Referência.

24.3.7. Será aplicada multa de 0,25% (vinte e cinco centésimos por cento) à 10% (dez por cento) do valor total do respectivo Pedido de Compras / Contrato pelo inadimplemento contratual relacionado às situações não previstas nos subitens anteriores.

24.3.8. As multas constantes nesse item poderão ser aplicadas cumulativamente conforme o caso e são meramente moratórias, não isentando a CONTRATADA o ressarcimento por perdas e danos pelos prejuízos a que der causa.

24.3.9. Caso o valor total pago mensalmente pela CONTRATANTE para manutenção dos equipamentos seja insuficiente para o débito das multas devidas pela CONTRATADA no referido mês, o valor devido deverá ser descontado integralmente do valor caucionado em garantia do cumprimento das obrigações contratuais.

24.3.10. Ao término dos prazos previstos, contados a partir da emissão da Ordem de Serviço, poderá ser aplicada multa moratória de 0,50% (cinquenta centésimos por cento), em cima do valor de cada item avaliado, por dia de atraso.

24.3.11. Rescisão unilateral do contrato no caso de reincidência.

24.3.12. Pela rescisão do contrato por iniciativa da CONTRATADA, sem justa causa, responderá esta por perdas e danos que a rescisão ocasionar ao SESI/CN.

24.3.13. Suspensão temporária do direito de participar em licitações e impedimento de contratar com o SESI/CN, por prazo não superior a 2 (dois) anos.

24.4. As multas serão descontadas dos pagamentos a que a CONTRATADA fizer jus, ou recolhidas diretamente à Tesouraria do SESI/CN, no prazo de 15 (quinze) dias, contados a partir da data de sua comunicação, ou, ainda, quando for o caso, cobradas judicialmente.

24.5. Para a aplicação das penalidades aqui previstas, a CONTRATADA será notificada para apresentação de defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir da notificação.

24.6. As penalidades previstas neste contrato são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis, tantas vezes quantas forem as irregularidades constatadas.

24.7. A CONTRATADA deverá comunicar ao SESI/CN, por escrito e justificadamente, as ocorrências de caso fortuito ou de força maior impeditivas do cumprimento do objeto contratado, no prazo máximo improrrogável de 2 (dois) dias úteis, contados da data da ocorrência, sob pena de não poder alegá-los posteriormente.

25. DAS DISPOSIÇÕES GERAIS

25.1. O SESI/CN não admitirá declarações posteriores ao recebimento dos envelopes de "proposta de preços" e "documentação de habilitação", de desconhecimento de fatos, no todo ou em parte, nem juntadas de documentos fora das datas especificadas neste Edital, que dificultem ou impossibilitem o julgamento das propostas ou a adjudicação à licitante vencedora.

25.2. São partes integrantes deste Edital os seguintes Anexos:

- ANEXO I – Termo de Referência;
- ANEXO II - Formulário de Proposta de Preços;
- ANEXO III - Minuta de Contrato de Prestação De Serviços.

25.3. É facultado à Pregoeira, em qualquer fase da licitação, promover diligência destinada a esclarecer ou a complementar a instrução do processo, vedada inclusão posterior de documento ou informação que deveria constar originariamente na "PROPOSTA DE PREÇOS" e na "DOCUMENTAÇÃO DE HABILITAÇÃO".

25.4. Os empregados e prepostos da empresa contratada não terão qualquer vínculo empregatício com o SESI/CN, correndo por conta exclusiva da licitante Contratada todas as obrigações decorrentes das legislações trabalhista, previdenciária, fiscal, tributária e comercial, as quais a licitante contratada se obriga a saldar na época devida.

25.5. É facultado ao SESI/CN, quando a convocada não assinar a Contrato de Prestação de Serviços, dentro do prazo máximo previsto neste Edital, convocar as licitantes remanescentes, observadas a ordem de classificação para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira classificada, inclusive quanto aos preços ou ainda cancelar a licitação.

25.6. Fica assegurado ao SESI/CN o direito de revogar ou cancelar a presente licitação mediante justificativa, antes da assinatura do Instrumento Contratual, sem que, em decorrência dessa medida tenham as licitantes direito à indenização, à compensação ou à reclamação de qualquer natureza.

25.7. A Pregoeira, a qualquer tempo, antes da data de apresentação das propostas, poderá proceder às alterações concernentes a esta licitação e/ou prorrogar a data de abertura do certame, divulgando o correspondente adendo e/ou adiamento no site https://conselhonacionaldosesi.org.br/transparencia/editais-e-licitacoes/ e no portal de compras do Governo Federal, www.gov.br/compras/pt-br

25.8. É facultado à Pregoeira suspender a sessão sempre que necessário.

25.9. As decisões referentes a este Pregão serão divulgados no site https://conselhonacionaldosesi.org.br/transparencia/editais-e-licitacoes/ e no portal de compras do Governo Federal, www.gov.br/compras/pt-br, sendo de inteira responsabilidade da licitante o acompanhamento da divulgação de cada fase.

25.10. O foro da Circunscrição Especial Judiciária de Brasília, Distrito Federal, será o competente para dirimir as questões oriundas desta Licitação e da relação jurídica dela decorrente.

Os casos omissos deste Edital serão resolvidos pela Pregoeira e pela Equipe de Apoio, com aplicação das disposições contidas no Regulamento de Licitações e Contratos do SESI.

Brasília, 16 de abril de 2021.

PEDRO ANTONIO FIORAVANTE SILVESTRE NETO
Superintendente Executivo
Conselho Nacional do SESI

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N° 02/2021
SESI – CONSELHO NACIONAL

ANEXO I
TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de empresa especializada para fornecimento de Solução Integrada de Serviços Gerenciados de Segurança que contemplem serviços de segurança de perímetro com fornecimento de equipamentos, administração e monitoração de segurança, resposta a incidentes de segurança e transferência de conhecimento para a equipe técnica do Conselho Nacional do SESI, conforme as especificações técnicas constantes neste Termo de Referência e em seus respectivos Anexos, adiante discriminadas:

ITEM	CÓDIGO	DESCRIÇÃO	QUANT.	UNID.	TIPO	VALOR MENSAL	VALOR TOTAL
1	27014	Solução Integrada de Serviços Gerenciados de Segurança	12	Mês	Despesa (serviço)	R$ 30.716,67	R$ 368.600,00
						VALOR MÁXIMO ACEITÁVEL:	**R$ 368.600,00**

OBS: Havendo qualquer discordância entre a descrição e a unidade de medida do CATSER e a do Edital, prevalecerá a descrição e unidade de medida constante no Edital.

1.2. Valor máximo aceitável da licitação **R$ 368.600,00 (trezentos e sessenta e oito mil e seiscentos reais)**.

2. JUSTIFICATIVA

2.1. A infraestrutura de Tecnologia da Informação (TI) abrange recursos e serviços que viabilizam as atividades do Conselho Nacional do Serviço Social da Indústria (CNSESI).

2.2. A contratação aqui prevista tem como finalidade garantir a continuidade e prover a segurança dos serviços de TI que suportam as atividades inerentes à missão organizacional.

2.3. No início do ano de 2020 o Conselho sofreu 2 ataques de *Ransonware* que culminaram na indisponibilidade de todos os serviços de TI pelo período de mais de uma semana em cada ataque.

2.4. A realização de todos os procedimentos que visam garantir a segurança dos dados e informações do Conselho precisam ser contínuos e são necessários para mitigarmos os riscos de novas infecções, o que exige uma grande carga horária da pequena equipe de TI.

2.5. O Conselho não possui Firewall - uma barreira de proteção em redes de computadores para controlar e filtrar o fluxo de dados entre um link da internet e a rede interna, evitando o roubo de informações e de execução de softwares com comportamentos suspeitos. Seu objetivo é permitir aplicação de políticas de segurança para que haja somente a transmissão e a recepção de dados autorizados.

2.6. A contratação em tela visa a prestação de serviços de detecção e respostas a incidentes de segurança da informação.

2.7. Ressalta-se como prioridade para a área de TI, que os acessos aos serviços, dados e informações do CN-SESI, externos a rede local, sejam controlados e protegidos para assegurar a confiabilidade, integridade e disponibilidade.

2.8. Garantia de 12 meses para todos os componentes de hardware e software. A CONTRATADA ficará encarregada de realizar alterações nas configurações do ambiente sempre que solicitado pelo Conselho, durante toda a vigência do contrato.

2.9. A assistência técnica e os serviços de sustentação serão executados durante o período de 12 meses, com atendimento on-site (nas dependências da CONTRATANTE), sempre que solicitado. O Conselho poderá, conforme sua necessidade, abrir chamados de suporte com a CONTRATADA e esta, sempre que necessário, poderá abrir chamado com os fabricantes que compõem a solução contratada.

3. DESCRIÇÃO GERAL

3.1. A contratação de serviços gerenciados de segurança deverá contemplar, no mínimo:

3.1.1. Uma solução de Segurança de Prevenção de Ameaças de próxima geração composta por um par de equipamentos (appliances) em regime de alta disponibilidade (cluster), construídos especificamente para exercer as funções de segurança de perímetro e prevenção de ameaças de próxima geração solicitadas neste Termo de Referência, com hardware e software;

3.1.2. Capacidades para suportar os serviços entregues e que, no momento de contingência ou indisponibilidade de um equipamento ou software, os produtos alocados suportem, sem degradação ou perda de performance, todos os requisitos técnicos exigidos;

3.1.3. Serviços Técnicos Especializados em regime 24x7X365 (vinte e quatro horas por dia durante sete dias na semana por trezentos e sessenta e cinco dias no ano) para gerenciamento, administração, suporte técnico, monitoramento de segurança, respostas aos incidentes de segurança e consultoria técnica;

3.1.4. Elementos dedicados para execução do Monitoramento de Segurança (SOC);

3.1.5. Garantias que permitam a manutenção do correto funcionamento e atualização da solução como um todo, visando minimizar os riscos inerentes ao negócio e à infraestrutura tecnológica da CONTRATADA;
3.1.6. Repasse de conhecimento para o corpo técnico da CONTRATANTE, visando permitir o alcance de todo o potencial desta contratação.
3.1.7. Operação assistida na primeira semana de execução dos serviços, visando familiarizar o corpo técnico do Conselho com as especificidades da solução implantada, além de fazer os ajustes finos necessários logo após a implementação.

3.2. A Solução de Prevenção de Ameaças de próxima geração deverá suportar e integrar nativamente diversas camadas tecnológicas de Segurança, todas do mesmo fabricante, constituindo um ambiente de defesa de perímetro cibernético eficiente e, ao mesmo tempo, consolidado:

3.2.1. Firewall de Próxima Geração;
3.2.2. Controle por Política de Firewall;
3.2.3. Controle de Aplicações;
3.2.4. Filtro de URL;
3.2.5. Análise de Malwares Modernos;
3.2.6. Prevenção de Ameaças;
3.2.7. Identificação de Usuários;
3.2.8. Filtro de Dados;
3.2.9. VPN Site-to-Site e Client-to-Site;
3.2.10. Quality Of Service;
3.2.11. Geo-Localização;
3.2.12. Console de Gerência;

3.3. A Solução e suas camadas devem sempre operar obrigatoriamente em modos de inspeção total, não sendo aceitos métodos dinâmicos, otimizados ou inteligentes, que apenas visam o desempenho e não a segurança do ambiente;

3.4. Deverá obrigatoriamente inspecionar todo o tráfego que a ela for direcionado, independentemente da direção ou condição;

3.5. Não deverá possuir limitação lógica de armazenamento e nem de recebimento de logs;

3.6. Deve ser integrada com serviço de diretório para correta identificação e autenticação dos usuários, sem a necessidade de instalação de agentes ou clientes nos servidores de diretórios ou máquinas de trabalho;

3.7. Deve auxiliar e facilitar a sua administração através de ferramentas que forneçam recomendações e melhores práticas em segurança, inclusive com alertas de erros comuns de configuração nas políticas e também no sistema operacional da solução.

3.8. Deve ser possível também verificar se as recomendações fornecidas estão sendo seguidas ou não;

3.9. Toda a solução deverá permitir o monitoramento de segurança, devendo estar integrada de forma a gerar alertas em tempo real das ameaças, dos incidentes e eventos de Segurança detectados.

3.10. A Solução de Prevenção de Ameaças de próxima geração deverá fornecer segurança cibernética de forma abrangente em um modelo de múltiplas camadas. Os elementos integrantes destas camadas geram uma grande quantidade de informações que devem ser tratadas e monitoradas constantemente, de forma a permitir que a CONTRATADA tenha visibilidade e controle total do seu ambiente.

3.11. O elemento de gerenciamento deverá se comunicar com todas as camadas da solução e suportar a integração de todos os seus resultados, configurações, informações, logs e eventos, de forma a permitir:

3.11.1. Visualização da situação atual e histórica da Segurança do ambiente;
3.11.2. Visualização e tomadas de decisão com base em referenciamento geográfico das informações de Segurança (ataques, invasões, conexões, etc.);
3.11.3. Relatórios de visões correlacionadas envolvendo as camadas de segurança da solução ofertada;
3.11.4. Relatórios de utilização dos recursos monitorados e protegidos;
3.11.5. Relatórios sumarizados, em formatos textuais e gráficos, que permitam o aprofundamento (drill down) nas análises;
3.11.6. Customização de relatórios e gráficos;
3.11.7. Exportação e também a visualização em tempo real dos relatórios;
3.11.8. Detectar e alertar acessos de administradores em horários irregulares e possíveis tentativas de adivinhação de credenciais administrativas (password guessing attacks) da solução;
3.11.9. Análises e alertas de alterações em configurações da solução antes que elas sejam aplicadas, visando impedir erros humanos de configuração;
3.11.10. Análises de risco do ambiente em tempo real, com base em melhores práticas de segurança, regulamentações e também em padrões customizados pela CONTRATADA;
3.11.11. Notificações instantâneas sobre mudanças, eventos e acontecimentos que representem ou gerem impacto na segurança do ambiente;
3.11.12. Referência cruzada da base de assinaturas de detecção com os identificadores CVE (Common Vulnerabilities and Exposures).

4. REQUISITOS BÁSICOS PARA EXECUÇÃO DOS SERVIÇOS

4.1. O serviço gerenciado de SOC consiste na sustentação, gerência, monitoramento e correções das soluções de Segurança impostas na execução dos serviços solicitados;

4.2. A CONTRATADA terá acesso via VPN, ou outra tecnologia equivalente, a console de gerenciamento centralizado para as atividades solicitadas e toda a parte de gerência e monitoramento da solução;
4.3. Será de responsabilidade da CONTRATADA o gerenciamento completo da solução de Segurança.

4.4. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade;

4.5. Todos os elementos que integram a Solução de Prevenção de Ameaças de próxima geração e suas camadas devem:

4.5.1. Todos os equipamentos necessários à prestação dos serviços devem ser novos e de primeiro uso. Além disso, devem ser entregues em suas embalagens originais, em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos;
4.5.2. Ser entregues equipamentos e softwares que não constem, no momento da apresentação da proposta técnica, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida. Não serão aceitas migrações futuras de plataformas, durante a vigência do contrato, pelo motivo de descontinuidade dos produtos;
4.5.3. Englobar a alocação de equipamentos e softwares necessários à consecução das atividades durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos em regime 24x7X365 (vinte e quatro horas por dia durante sete dias na semana por trezentos e sessenta e cinco dias no ano);
4.5.4. Ser instalados em sua versão mais estável, atualizada e estar coberto por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante. A comprovação se dará por meio da interface de gerenciamento dos equipamentos e softwares fornecidos;
4.5.5. Ser otimizado para análises de conteúdo de aplicações e ameaças de próxima geração;
4.5.6. Possuir sistema operacional customizado pelo próprio fabricante da Solução para garantir segurança e melhor desempenho, permitindo o monitoramento nativo de seus recursos;
4.5.7. Suportar monitoramento através de SNMP v1, v2 e v3;
4.5.8. Suportar gerenciamento através de protocolos seguros como uma Console Dedicada, Linha de Comando (CLI) via SSH e interface Web via HTTPS;
4.5.9. Utilizar canais criptografados para se comunicar com os demais elementos da Solução, sendo que a criptografia deve ser implantada através de uma Infraestrutura de Chaves Públicas interna da própria Solução ofertada;
4.5.10. Integrar com serviços de diretório (Active Directory) sem a necessidade de instalação de agentes de qualquer natureza, visando a correta identificação de Usuários,

Grupos e suas funções para fornecer a granularidade necessária na administração de uma solução deste tipo;
4.5.11. No caso de usuários não registrados ou não reconhecidos pelo domínio, deve ser fornecida uma possibilidade de autenticação baseada em navegador (Captive Portal);
4.5.12. Identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento;
4.5.13. Permitir auditoria e relatórios avançados das alterações realizadas;
4.5.14. O par de equipamentos devem ser idênticos para serem configurados em regime de Alta Disponibilidade e devem possuir, cada um, no mínimo:
4.5.14.1. Throughput de 480 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
4.5.14.2. Throughput de 250 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes:
4.5.14.2.1. Controle de aplicação IPS;
4.5.14.2.2. Antivírus e Antispyware;
4.5.14.2.3. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
4.5.14.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará a CONTRATANTE o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital;
4.5.14.4. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas no Regulamento de Licitações e Contrato do SESI;
4.5.14.5. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend);
4.5.14.6. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4;
4.5.14.7. Suporte a, no mínimo, 60.000 conexões simultâneas;
4.5.14.8. Suporte a, no mínimo, 3.000 novas conexões por segundo;
4.5.14.9. Fonte redundante interna ou externa: 120/240 AC ou DC;
4.5.14.10. Disco de, no mínimo, 30 GB;
4.5.14.11. No mínimo, 05 (cinco) interfaces de rede 10/100/1000 base-TX;
4.5.14.12. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;
4.5.14.13. 1 (uma) interface do tipo console ou similar;
4.5.14.14. Suporte a, no mínimo, 10 (dez) zonas de segurança;
4.5.14.15. Estar licenciada para ou suportar sem o uso de licença, 100 (cem) clientes de VPN SSL simultâneos;
4.5.14.16. Estar licenciada para ou suportar sem o uso de licença, 100 (cem) túneis de VPN IPSEC simultâneos;
4.5.14.17. Cada unidade que compõe a camada de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

4.5.14.18. Por console de gerência e monitoramento, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

4.6. EXECUÇÃO DOS SERVIÇOS

4.6.1. A solução deve possuir características de proteção de rede com funcionalidades de Segurança e console de gerência e monitoração;
4.6.2. Por funcionalidades de Segurança entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
4.6.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação, de tecnologia e disponibilidade;
4.6.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
4.6.5. Os hardwares e softwares que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração;
4.6.6. Caso a CONTRATADA opte em entregar servidores com sistemas operacionais genéricos para atender a demanda, o mesmo estará sujeito a teste de desempenho;
4.6.6.1. Caso ocorra a necessidade de teste de desempenho, a CONTRATANTE se reserva no direito de testar, sempre que necessário, o servidor, de modo que o mesmo só será aceito quando demonstrado que atinge todas as expectativas quanto às funcionalidades de software e hardware solicitadas neste termo técnico;
4.6.7. Todos softwares fornecidos pela CONTRATADA deverão ser entregues e mantidos em suas versões mais atualizadas durante toda a vigência do contrato;
4.6.8. Os softwares de antivírus e EDR fornecidos pela CONTRATANTE deverão ser mantidos atualizados nos equipamentos e monitorados constantemente;
4.6.9. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
4.6.9.1. Suporte a 4094 VLAN Tags 802.1q;
4.6.9.2. Policy based routing ou policy based forwarding;
4.6.9.3. Roteamento multicast (PIM-SM);
4.6.9.4. DHCP Relay;
4.6.9.5. DHCP Server;
4.6.9.6. Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
4.6.9.7. Suportar sub-interfaces ethernet lógicas.
4.6.9.8. Suporte a, no mínimo, 3 (três) roteadores virtuais na mesma instância de firewall;
4.6.10. Deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação, a solução deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

4.6.11. Deve suportar os seguintes tipos de NAT:
4.6.11.1. NAT dinâmico (Many-to-1);
4.6.11.2. NAT dinâmico (Many-to-Many);
4.6.11.3. NAT estático (1-to-1);
4.6.11.4. NAT estático (Many-to-Many);
4.6.11.5. NAT estático bidirecional 1-to-1;
4.6.11.6. Tradução de porta (PAT);
4.6.11.7. NAT de Origem;
4.6.11.8. NAT de Destino;
4.6.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
4.6.12. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
4.6.13. Deve implementar o protocolo ECMP;
4.6.14. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;
4.6.15. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de troubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
4.6.16. Enviar log para sistemas de monitoração externos, simultaneamente;
4.6.17. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
4.6.18. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
4.6.19. Proteção contra anti-spoofing;
4.6.20. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
4.6.21. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
4.6.22. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver descriptografia de SSL e SSH;
4.6.23. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.6.24. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
4.6.25. Suportar a OSPF graceful restart;
4.6.26. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
4.6.27. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

4.6.28. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de segurança, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
4.6.29. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
4.6.30. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
4.6.31. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
4.6.32. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
4.6.33. Suporte à configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
4.6.34. Em modo transparente;
4.6.35. Em layer 3;
4.6.36. A configuração em alta disponibilidade deve sincronizar:
4.6.36.1. Sessões;
4.6.36.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
4.6.36.3. Certificados decriptografados;
4.6.36.4. Associações de Segurança das VPNs;
4.6.36.5. Tabelas FIB;
4.6.36.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
4.6.37. Tal necessidade se faz necessária para a migração ou continuidade da plataforma de segurança após o término do contrato.

4.7. CONTROLE POR POLÍTICA

4.7.1. Deverá suportar controles por zona de segurança.
4.7.2. Controles de políticas por porta e protocolo.
4.7.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
4.7.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
4.7.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;
4.7.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
4.7.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência;
4.7.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
4.7.9. Controle, inspeção e descriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

4.7.10. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
4.7.11. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
4.7.12. Controle de inspeção e descriptografia de SSH por política;
4.7.13. A descriptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
4.7.14. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
4.7.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
4.7.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
4.7.17. Suporte a objetos e regras IPV6.
4.7.18. Suporte a objetos e regras multicast.
4.7.19. Deve suportar no mínino três tipos de negação de tráfego nas políticas: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
4.7.20. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.8. CONTROLE DE APLICAÇÕES

4.8.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
4.8.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.8.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;
4.8.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;
4.8.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

4.8.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.
4.8.7. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
4.8.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;
4.8.9. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;
4.8.10. Deve permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, etc;
4.8.11. Identificar o uso de táticas evasivas via comunicações criptografadas;
4.8.12. Atualizar a base de assinaturas de aplicações automaticamente;
4.8.13. Reconhecer aplicações em IPv6;
4.8.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseada no IP de origem, usuários e grupos do LDAP/AD;
4.8.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
4.8.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
4.8.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;
4.8.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.8.19. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da CONTRATANTE;
4.8.20. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
4.8.20.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

4.8.21. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
4.8.22. Deve alertar o usuário quando uma aplicação for bloqueada;
4.8.23. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
4.8.24. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:
4.8.24.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
4.8.24.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da aplicação na determinada regra;
4.8.24.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
4.8.24.4. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
4.8.24.5. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;
4.8.24.6. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;
4.8.24.7. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;
4.8.25. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
4.8.25.1. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).
4.8.25.2. Nível de risco da aplicação.
4.8.25.3. Categoria e sub-categoria de aplicações.
4.8.25.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

4.9. PREVENÇÃO DE AMEAÇAS

4.9.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados ou entregue através de composição com outro equipamento ou fabricante.
4.9.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
4.9.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware:
4.9.4.1. Permitir;
4.9.4.2. Permitir e gerar log;
4.9.4.3. Bloquear;

4.9.4.4. Bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
4.9.5. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2;
4.9.6. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
4.9.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
4.9.8. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
4.9.9. Deve permitir o bloqueio de vulnerabilidades.
4.9.10. Deve permitir o bloqueio de exploits conhecidos.
4.9.11. Deve incluir proteção contra a ataques de negação de serviços.
4.9.12. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;
4.9.13. Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.9.13.1. Análise de padrões de estado de conexões;
4.9.13.2. Análise de decodificação de protocolo;
4.9.13.3. Análise para detecção de anomalias de protocolo;
4.9.13.4. Análise heurística;
4.9.13.5. IP Defragmentation;
4.9.13.6. Remontagem de pacotes de TCP;
4.9.13.7. Bloqueio de pacotes malformados.
4.9.13.8. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
4.9.14. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
4.9.15. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
4.9.16. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
4.9.17. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
4.9.18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.9.19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
4.9.20. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.9.21. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.9.22. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

4.9.24. Suportar bloqueio de arquivos por tipo;
4.9.24. Identificar e bloquear comunicação com botnets;
4.9.25. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);
4.9.26. Deve suportar referência cruzada com CVE;
4.9.27. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
4.9.28. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
4.9.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;
4.9.30. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
4.9.31. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.9.32. Os eventos devem identificar o país de onde partiu a ameaça;
4.9.33. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
4.9.34. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.
4.9.35. Rastreamento de vírus em pdf.
4.9.36. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
4.9.37. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.10. ANÁLISE DE MALWARES MODERNOS

4.10.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
4.10.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
4.10.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
4.10.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características

indesejáveis como softwares que deixam o sistema operacional lento, que alteram parâmetros do sistema, etc.;
4.10.5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
4.10.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional, Windows 7 (32 bits) e Windows 7 (64 bits), ou superior;
4.10.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
4.10.8. Para ameaças trafegadas em protocolo SMTP ou POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
4.10.9. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);
4.10.10. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;
4.10.11. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;
4.10.12. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
4.10.13. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
4.10.14. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falsopositivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.
4.10.15. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;
4.10.16. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
4.10.17. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
4.10.18. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox;
4.10.19. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox com frequência de, pelo menos, 5 minutos
4.10.20. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

4.10.21. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

4.11. FILTRO DE URL

4.11.1. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.11.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.
4.11.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.
4.11.4. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
4.11.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
4.11.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
4.11.7. Suporta base ou cache de URLs local no appliance, evitando atraso de comunicação/validação das URLs;
4.11.8. Possui pelo menos 60 categorias de URLs;
4.11.9. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;
4.11.10. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;
4.11.11. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
4.11.12. Suporta a criação categorias de URLs customizadas;
4.11.13. Suporta a exclusão de URLs do bloqueio, por categoria;
4.11.14. Permite a customização de página de bloqueio;
4.11.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução;
4.11.16. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
4.11.17. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
4.11.18. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

4.12. IDENTIFICAÇÃO DE USUÁRIOS

4.12.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
4.12.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
4.12.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
4.12.4. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;
4.12.5. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
4.12.6. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;
4.12.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
4.12.8. Suporte a autenticação Kerberos;
4.12.9. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
4.12.10. Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;
4.12.11. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;
4.12.12. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
4.12.13. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

4.13. QUALIDADE DE SERVIÇO (QoS)

4.13.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.13.2. Suportar a criação de políticas de QoS por:
4.13.2.1. Endereço de origem
4.13.2.2. Endereço de destino
4.13.2.3. Por usuário e grupo do LDAP/AD.
4.13.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
4.13.2.5. Por porta;
4.13.2.6. O QoS deve possibilitar a definição de classes por:
4.13.2.7. Banda Garantida
4.13.2.8. Banda Máxima
4.13.2.9. Fila de Prioridade.
4.13.3. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
4.13.4. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
4.13.5. Disponibilizar estatísticas RealTime para classes de QoS.
4.13.6. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.14. FILTRO DE DADOS

4.14.1. Permite a criação de filtros para arquivos e dados pré-definidos;
4.14.2. Os arquivos devem ser identificados por extensão e assinaturas;
4.14.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre protocolos HTTP, HTTPs, FTP, SMTP e SMB;
4.14.4. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.14.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
4.14.6. Permitir listar o número de aplicações suportadas para controle de dados;
4.14.7. Permitir listar o número de tipos de arquivos suportados para controle de dados;

4.15. GEO-LOCALIZAÇÂO

4.15.1. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejam bloqueados.
4.15.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
4.15.3. Deve possibilitar a utilização de informações geográficas para criar políticas.

4.16. VIRTUAL PRIVATE NETWORK Site-Site e Client-to-Site

4.16.1. Suportar VPN Site-to-Site e Cliente-To-Site;
4.16.2. Suportar IPSec VPN;

4.16.3. Suportar SSL VPN;
4.16.4. A VPN IPSEc deve suportar:
4.16.4.1. 3DES;
4.16.4.2. Autenticação MD5 e SHA-1;
4.16.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
4.16.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
4.16.4.5. AES 128~~, 192~~ e 256 (Advanced Encryption Standard)
4.16.4.6. Autenticação via certificado IKE PKI.
4.16.5. Deve possuir interoperabilidade com os seguintes fabricantes:
4.16.5.1. Cisco;
4.16.5.2. Checkpoint;
4.16.5.3. Juniper;
4.16.5.4. Palo Alto Networks;
4.16.5.5. Fortinet;
4.16.5.6. Sonic Wall;
4.16.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
4.16.7. A VPN SSL deve suportar:
4.16.7.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.16.7.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.16.7.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;
4.16.7.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
4.16.8. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
4.16.9. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
4.16.10. Atribuição de DNS nos clientes remotos de VPN;
4.16.11. A solução de VPN deve verificar se o cliente que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
4.16.12. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
4.16.13. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
4.16.14. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
4.16.15. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
4.16.16. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

4.16.17. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
4.16.18. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
4.16.19. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
4.16.20. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
4.16.21. Suporta leitura e verificação de CRL (certificate revocation list);
4.16.22. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
4.16.23. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
4.16.24. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,
4.16.25. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
4.16.25.1. Antes do usuário autenticar na estação;
4.16.25.2. Após autenticação do usuário na estação;
4.16.25.3. Sob demanda do usuário;
4.16.25.4. Deve manter uma conexão segura com o portal durante a sessão.
4.16.25.5. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx;
4.16.25.6. O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID) e sistemas operacionais Linux;
4.16.26. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;
4.16.27. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;
4.16.28. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;
4.16.29. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
4.16.30. Deve haver a opção de o cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
4.16.31. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

4.17. CONSOLE DE GERÊNCIA

4.17.1. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
4.17.2. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
4.17.3. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
4.17.4. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows ou Linux;
4.17.5. O gerenciamento deve permitir/possuir:
4.17.5.1. Criação e administração de políticas de firewall e controle de aplicação;
4.17.5.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
4.17.5.3. Criação e administração de políticas de Filtro de URL;
4.17.5.4. Monitoração de logs;
4.17.5.5. Ferramentas de investigação de logs;
4.17.5.6. Debugging;
4.17.5.7. Captura de pacotes.
4.17.5.8. Acesso concorrente de administradores;
4.17.6. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;
4.17.7. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
4.17.8. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;
4.17.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
4.17.10. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
4.17.11. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
4.17.12. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
4.17.13. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
4.17.14. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.17.15. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
4.17.16. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
4.17.17. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
4.17.18. Criação de regras que fiquem ativas em horário definido;
4.17.19. Criação de regras com data de expiração;
4.17.20. Backup das configurações e rollback de configuração para a última configuração salva;
4.17.21. Suportar Rollback de Sistema Operacional para a última versão local;
4.17.22. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
4.17.23. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
4.17.24. Validação de regras antes da aplicação;
4.17.25. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc;
4.17.26. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação;
4.17.27. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
4.17.28. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
4.17.29. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas;
4.17.30. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
4.17.31. Deve possibilitar a integração com outras soluções de SIEM de mercado (thirdparty SIEM vendors);
4.17.32. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
4.17.33. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
4.17.34. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
4.17.35. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
4.17.36. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

4.17.37. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
4.17.38. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela;
4.17.39. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
4.17.40. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;
4.17.41. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
4.17.42. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
4.17.43. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
4.17.44. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
4.17.45. Deve ser possível exportar os logs em CSV;
4.17.46. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
4.17.47. Rotação do log;
4.17.48. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
4.17.49. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
4.17.50. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
    4.17.50.1. Situação do dispositivo e do cluster;
    4.17.50.2. Principais aplicações;
    4.17.50.3. Principais aplicações por risco;
    4.17.50.4. Administradores autenticados na gerência da plataforma de segurança;
    4.17.50.5. Número de sessões simultâneas;
    4.17.50.6. Status das interfaces;
    4.17.50.7. Uso de CPU;
4.17.51. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
    4.17.51.1. Resumo gráfico de aplicações utilizadas;
    4.17.51.2. Principais aplicações por utilização de largura de banda de entrada e saída;
    4.17.51.3. Principais aplicações por taxa de transferência de bytes;
    4.17.51.4. Principais hosts por número de ameaças identificadas;

4.17.51.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

4.17.52. Deve permitir a criação de relatórios personalizados;

4.17.53. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

4.17.54. Gerar alertas automáticos via:

4.17.54.1. Email;

4.17.54.2. SNMP;

4.17.54.3. Syslog;

4.17.55. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

5. MONITORAMENTO E GERENCIAMENTO DE SEGURANÇA:

5.1. Deverá monitorar todos os elementos da Solução de Prevenção de Ameaças de próxima geração em regime 24x7x365;

5.2. Este serviço deverá utilizar também as ferramentas licenciadas pela CONTRATANTE, durante o período de vigência de contrato das mesmas. São elas:

5.2.1. Antivírus Bitdefender

5.2.2. EDR FIREEYE

5.3. A CONTRATANTE possui atualmente em seu parque computacional cerca de 80 (oitenta) ativos que deverão ser contemplados neste serviço;

5.4. A CONTRATADA será responsável por manter as ferramentas de antivírus e EDR em pleno funcionamento, a partir da instalação, atualização e monitoração dos ativos da CONTRATANTE;

5.5. A CONTRATADA deverá realizar o monitoramento da solução nas dependências da CONTRANTE, sempre que necessário.

5.6. A CONTRATADA deverá monitorar alertas gerados pela solução de Segurança, envolvendo atividades como:

5.6.1. Alta disponibilidade;

5.6.2. Atividades de Rede;

5.6.3. Atividades de Ameaças;

5.6.4. Atividades do Túnel Ipsec;
5.6.5. Falhas de interfaces dos equipamentos;
5.6.6. Consumo de link de internet;
5.6.7. Controle de Aplicações;
5.6.8. Detecções de Botnet;
5.6.9. Detecção de Hosts com acessos a domínios maliciosos;

5.7. Em eventos de monitoramento de alertas de segurança, onde o analista identificar certos indicadores de comportamento, que serão detalhados pela solução de Segurança, a CONTRATADA emitirá um relatório informativo de modo a dar visibilidade a CONTRATANTE de possíveis riscos associados ao evento.

5.8. O relatório somente será necessário se a solução indicar que o evento possui severidade crítica ou alta;

5.9. Em casos de incidentes ocorridos detectados em soluções terceiras, a CONTRATADA poderá ser acionada a fim de identificar algum registro do incidente na solução de Next Generation Firewall.

5.10. O monitoramento dos ativos do ambiente da CONTRATANTE deverá ser realizado através de ferramenta (hardware e/ou software) que coletarão as informações necessárias via agente ou sem agente para o monitoramento de segurança (SOC);

5.11. A solução de monitoramento utilizada deverá ser implementada no ambiente da CONTRATADA;

5.12. O acesso a solução de monitoramento deverá ser realizado apenas pela equipe de tecnologia da informação da CONTRATANTE e a equipe de serviço de SOC da CONTRATADA;

5.13. A solução de monitoramento dos ativos deve realizar:

5.13.1. Auto descoberta de servidores e dispositivos de rede;
5.13.2. Monitoração distribuída com a administração centralizada via WEB;
5.13.3. Suporte para mecanismo de pooling e trapping;
5.13.4. Autenticação segura de usuário;
5.13.5. Permissões flexíveis de usuário;
5.13.6. Interface baseada em web;
5.13.7. Notificação por e-mail flexível de eventos predefinidos;
5.13.8. Visualização em alto nível dos recursos monitorados a nível gerencial;
5.13.9. Auditoria;

5.14. O monitoramento de segurança deverá ser realizado através de ferramentas (hardware e/ ou software), que coletarão as informações necessárias para a execução do serviço de SOC;

5.15. O monitoramento deverá coletar informações a respeito do desempenho dos elementos monitorados, considerando, no mínimo:

5.15.1. Utilização de CPU;
5.15.2. Utilização de Memória RAM;
5.15.3. Utilização de Discos;
5.15.4. Performance de escrita e leitura de disco (I/O);
5.15.5. Vazão de dados (throughput) de rede;
5.15.6. Vazão de pacotes por segundo;
5.15.7. Conexões por segundo;
5.15.8. Conexões simultâneas;

5.16. O monitoramento deverá ser capaz de verificar a disponibilidade dos elementos monitorados através de, no mínimo, uma das seguintes formas:

5.16.1. ICMP (ping);
5.16.2. SNMP (v1, v2 e v3);
5.16.3. Serviços TCP;
5.16.4. Serviços UDP;

5.17. O monitoramento deverá ser capaz de coletar as informações de segurança (ameaças, ataques, intrusões, etc.) fornecidas pelos elementos monitorados e também do ambiente em questão, através de, no mínimo, uma das seguintes formas:

5.17.1. Syslog;
5.17.2. Syslog com TLS1.2;
5.17.3. Requisições SNMP;
5.17.4. Traps SNMP;
5.17.5. SSH;
5.17.6. REST API;

5.18. O monitoramento deverá ser capaz de coletar e reportar, minimamente, os seguintes itens da solução ofertada:

5.18.1. Estado das funcionalidades de segurança;
5.18.2. Estatísticas dos principais ataques, vírus e aplicações detectados;
5.18.3. Alertas de incidentes de segurança;
5.18.4. Versão instalada;
5.18.5. Atualizações disponíveis;

5.19. As informações monitoradas, detectadas ou coletadas deverão ser enviadas sempre de forma segura (comunicação criptografada) ao SOC;

5.20. O SOC deve ser capaz de comunicar automaticamente os alertas através de, no mínimo, as seguintes formas:

5.20.1. E-mail;
5.20.2. Mensagem SMS;
5.20.3. Portal de Monitoramento Web;
5.20.4. Ligação telefônica automática;
5.20.5. Sistema de mensagem instantânea (WhatsApp ou Telegram)

5.21. O SOC deverá suportar a abertura de solicitações de atendimento através dos seguintes canais:

5.21.1. Número de telefone gratuito (0800);
5.21.2. E-mail;
5.21.3. Portal de atendimento WEB;

5.22. O SOC deverá possuir controle de acesso físico, onde apenas funcionários autorizados possuem acesso;

5.23. O SOC deverá possuir monitoramento através de vídeo 24x7 (CFTV), de forma a comprovar o seu funcionamento e também o acesso de apenas funcionários autorizados;

5.23.1. Filmar toda a área do Datacenter de infraestrutura da CONTRATADA, mantendo as imagens armazenadas por no mínimo 90 (noventa) dias.

5.24. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operação de Segurança da Informação.

5.25. Caso algum dos serviços de gerenciamento e monitoramento não seja realizado no mesmo espaço físico que o de Centro de Operação de Segurança da Informação, todos os requisitos devem ser atendidos.

5.26. Possuir sistema de climatização de modo a garantir as corretas condições térmicas para os equipamentos no ambiente da infraestrutura física.

5.27. A CONTRATADA deverá emitir registros de todas as intervenções realizadas, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos e detalhados das ocorrências e também subsidiar as decisões da contratante.

5.28. A CONTRATADA será responsável por implementar e apoiar o processo de Resposta a Incidentes de Segurança.

5.28.1. Deverá avaliar situações em que o ambiente esteja sob ataque ou risco iminente de ataque, provendo o conhecimento e experiência necessários para as medidas de preparação, mitigação, contenção, defesa e resposta apropriadas;

5.29. A CONTRATADA será responsável por implementar os procedimentos destinados a prevenir a ocorrência de erros e defeitos nos serviços, dentre quaisquer outras atividades de conservação das soluções e do ambiente, de acordo com as recomendações, melhores práticas e normas técnicas específicas para os recursos utilizados;
5.30. A CONTRATADA será responsável por implementar os procedimentos de ajuste (*tunning*) para manter os serviços e as soluções contempladas na contratação em sua melhor forma de utilização;

5.31. A CONTRATADA será responsável por implementar os procedimentos de Threat Hunting e acompanhamento periódico do ambiente para identificar possíveis comprometimentos de segurança;

5.32. Deverão ser realizadas reuniões mensais gerenciais para avaliação e acompanhamento dos serviços contratados;
5.33. Deverão ser realizadas reuniões técnicas para planejamento e execução de serviços com vistas à melhoria do ambiente instalado, sempre que necessária ou solicitada pela CONTRATANTE;

5.34. Deverão ser realizadas revisões e análises técnicas pelo menos a cada 2 (dois) meses ou sempre que necessário;

6. OPERAÇÃO ASSISTIDA

6.1. A CONTRATADA deverá incluir operação assistida, mediante alocação de, no mínimo, 1 (um) profissional, após implementação do serviço gerenciado e SOC, durante 1 (uma) semana, a contar da data do recebimento pela CONTRATADA da Autorização para Início dos Serviços, perfazendo 8 (oito) horas diárias, nas dependências da CONTRATANTE visando familiarizar o corpo técnico do Conselho com as especificidades da solução implantada, além de fazer os ajustes finos necessários logo após a implementação.

6.2. A CONTRATADA, se acionada no período de operação assistida, deverá gerar relatórios de processos, incluindo sua análise.

6.3. O prazo máximo para criação de novos relatórios, processos e análises não poderá exceder a 5 (cinco) dias úteis.

7. REPASSE DE CONHECIMENTO

7.1. A contratada deverá fornecer repasse de conhecimento da solução ofertada e também da operação dos serviços contratados;

7.2. Todo o conteúdo, material didático, infraestrutura de aula e de laboratórios para atividades práticas devem ser adequados para cumprir os objetivos do repasse;

7.3. O repasse de conhecimento deve ser realizado no período de 10 dias após finalização do processo de implantação do serviço de SOC e solução;

7.4. O repasse de conhecimento deve ser realizado nas dependências da CONTRATADA ou de forma remota e deverá oferecer todos os recursos necessários para realizar a atividade;

7.5. Caso o treinamento seja realizado fora de Brasília, quaisquer custos com passagem, hospedagem e alimentação deverá ser de responsabilidade da CONTRATADA;

7.6. A turma deverá comportar até 4 alunos;

7.7. Os treinamentos deverão ser de, no mínimo, 24 horas;

8. NÍVEIS DE ACORDO DE SERVIÇO

8.1. A CONTRATANTE, durante toda a vigência contratual, poderá abrir chamados ilimitados para o suporte técnico;
8.2. A contratada assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio da CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da execução demandadas pela contratante.

8.3. Toda e qualquer atividade referente a configurações, ajustes, e outras parametrizações, que ocorrerem posteriormente à fase de implantação, serão precedidas da abertura de um chamado técnico.

8.4. Caso a atividade ocorra de modo proativo, a CONTRATADA informará a CONTRATANTE o motivo da execução tempestiva das ações através de e-mail;

8.5. Nos casos em que alguma atividade do serviço necessite da parada da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda com a autorização, ou para que seja agendada nova data, a ser definida pela CONTRATANTE.

8.6. Todas as atualizações que envolvam indisponibilidade do ambiente, devem ser agendadas com a equipe técnica da CONTRATANTE.

8.7. A CONTRATADA deverá possuir Central de Atendimento em português (brasileiro) para abertura de chamados e demais comunicações pertinentes, em regime 24x7x365;

8.8. A CONTRATANTE poderá solicitar a execução de serviços específicos através de canais de comunicação, como:

8.8.1. E-mail;
8.8.2. Contato Telefônico via 0800;
8.8.3. Sistema de Chamados Web;

8.8.4. O sistema de abertura de chamados deverá possuir um identificador único para cada solicitação de atendimento;
8.8.5. A CONTRATANTE considerará efetivamente realizado o serviço quando houver confirmação por sua área técnica da conclusão satisfatória do atendimento;
8.8.6. Todas as solicitações técnicas somente poderão ser encerradas com a anuência da CONTRATADA e do CONTRATANTE;
8.8.7. A CONTRATADA manterá cadastro das pessoas indicadas pelo CONTRATANTE que poderão efetuar a abertura e fechamento das solicitações de serviço;

8.9. Todo atendimento técnico presencial deverá ser registrado através de relatórios técnicos detalhados;

8.10.O término do atendimento não poderá ultrapassar o prazo estipulado para os diferentes níveis de criticidade;

8.11. Caso a CONTRATADA não cumpra com os prazos estipulados, ela estará passível às sanções administrativas cabíveis;

8.12. O chamado aberto junto à CONTRATADA, após fechado, poderá ser reaberto, se necessário a qualquer momento fazendo referência ao número original de identificação da chamada;

8.13. Considera-se suporte técnico On-Site as atividades que devem ser executadas de forma presencial e acompanhadas por funcionário da CONTRATANTE;

8.14. A CONTRATADA deverá iniciar o atendimento de acordo com os prazos estipulados para o nível de criticidade. O início do prazo para o atendimento é o mesmo para os tipos de suporte On-site e Remoto;

8.15. Os serviços de manutenção e suporte técnico poderão ser acionados a partir da data da assinatura do contrato;

8.16. A manutenção corretiva compreende os serviços para o restabelecimento do perfeito funcionamento dos equipamentos, com fornecimento de peças, de acordo com as especificações do fabricante, quando da ocorrência de quaisquer falhas ou defeitos nos componentes de hardware;

8.17. A Contratada deverá prestar os serviços de manutenção, com aparelhamento e ferramentas próprios, e técnicos com especialização, devidamente identificados;

8.18. Os serviços de manutenção serão prestados com atendimento presencial, on-site, e deverá cobrir todo e qualquer defeito apresentado, ajustes, reparos e correções necessárias para o perfeito estado de funcionamento da solução;

8.19. O suporte técnico consiste no restabelecimento do funcionamento correto das soluções cobertas por:

8.19.1. Esta contratação, assim como suas funcionalidades, através de um conjunto de ações e atividades (de configuração) que permitam a habilitação, a implementação/aplicação, a manutenção e a colocação em produção de quaisquer funcionalidades destes dispositivos.

8.20. Caso haja necessidade de atualização de firmware dos componentes, a CONTRATADA deve providenciar o pacote de software e efetuar o serviço de atualização.
8.21. Fica facultado à equipe técnica da CONTRATANTE o fornecimento de acesso remoto para atendimento do tipo suporte, em caso onde os problemas identificados permitam esse tipo de atuação.

8.22. Deverão ser emitidos relatórios mensais, e sempre que solicitado pelo CONTRATANTE, em arquivo eletrônico, preferencialmente nos formatos .XLS, .XLSX, .DOC, .DOCX ou .PDF, com informações analíticas dos serviços prestados no período, incluindo:

8.22.1. Quantidade de chamados registrados no período;
8.22.2. Número do chamado registrado e nível de severidade, inclusive aqueles com reabertura;
8.22.3. Data e hora de abertura (horário de Brasília/DF);
8.22.4. Data e hora de início e conclusão do atendimento (horário de Brasília/DF);
8.22.5. Consumo total de horas dos chamados no mês;
8.22.6. Identificação do técnico do CONTRATANTE que registrou o chamado;
8.22.7. Identificação do técnico da CONTRATADA que prestou o suporte técnico;
8.22.8. Descrição do problema;
8.22.9. Descrição da solução;
8.22.10. Informações sobre eventuais escalações;
8.22.11. Total de chamados no mês e o total acumulado até a apresentação do relatório.

8.23. A CONTRATADA deverá gerar e apresentar relatórios mensais, e quando solicitados pela CONTRATANTE, extraídos da solução de Next Generation Firewall, contendo, no mínimo, atividades detectadas conforme os itens abaixo:

8.23.1. Ameaças;
8.23.2. Filtro de Conteúdo Bloqueado;
8.23.3. Análises do Sandbox;
8.23.4. Acesso a VPN;
8.23.5. Falhas detectadas na solução;
8.23.6. Arquivos que foram analisados pela solução de Next Generation Firewall;

8.24. A CONTRATADA deverá disponibilizar painéis do tipo Dashboard de monitoramento da Segurança na CONTRATANTE;

8.25. A CONTRATADA deverá realizar a configuração de painéis e relatórios de monitoramento na solução fornecida, de modo a permitir o acompanhamento do status diário da solução pela CONTRATANTE.

8.26. A CONTRATADA deverá configurar um conjunto básico de painéis, contendo indicadores definidos de acordo com as bases específicas para monitoramento, podendo as mesmas serem customizadas para o ambiente da CONTRATANTE.

8.27. A contratada deverá emitir relatório mensal proativo com indicativos da saúde do ambiente e da solução de segurança;

8.28. PRAZO PARA SOLUÇÃO DAS OCORRÊNCIAS

8.28.1. Os níveis de severidade são descritos abaixo:

8.28.1.1. **Severidade 1** – quando ocorre a perda ou paralisação de serviços relevantes prestados pela **CONTRATANTE** ou atividades exercidas pela mesma, configurando-se como situação de emergência onde o atendimento deve ser realizado de forma presencial. Uma solicitação de serviço de **Severidade 1** pode possuir uma ou mais das seguintes características:

8.28.1.1.1. Equipamento corrompido;

8.28.1.1.2. Uma função crítica do equipamento não está disponível;

8.28.1.1.3. O equipamento se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos;

8.28.1.1.4. O equipamento falha repetidamente após tentativas de reinicialização;

8.28.1.1.5. Falha crítica de componente do equipamento.

8.28.1.2. **Severidade 2** – quando se verifica uma grave perda de funcionalidade, no entanto, sem interromper os serviços prestados pela **CONTRATANTE** ou atividades exercidas pela mesma.

8.28.1.3. **Severidade 3** – quando se verifica uma perda de menor relevância de funcionalidades, causando apenas inconveniências para a devida prestação dos serviços pela **CONTRATANTE** ou a realização de atividades exercidas pela mesma.

8.28.1.4. **Severidade 4** – quando solicitado criação de regras customizáveis nas soluções que não dependem de tal ação para a devida operação da CONTRATANTE ou atividades exercidas pela mesma.

8.28.1.5. **Severidade 5 -** quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades, porém sem prejudicar diretamente a devida prestação dos serviços pela **CONTRATANTE** ou a realização de atividades exercidas pela mesma.

8.28.2. O nível de severidade será atribuído pela CONTRATANTE no momento da abertura do chamado.

8.28.3. Para os chamados de **Suporte Técnico referentes às ocorrências de hardware**, deverão ser considerados os seguintes prazos de acordo com os níveis de severidade:

Tabela 01

SUPORTE TÉCNICO PARA OCORRÊNCIAS DE HARDWARE (a partir do registro da ocorrência)		
SEVERIDADE INFORMADA	**1º CONTATO COM A CONTRATANTE**	**TEMPO PARA SOLUÇÃO**
1	**15 minutos**	**2 horas corridas**
2	**30 minutos**	**4 horas corridas**
3	**60 minutos**	**24 horas corridas**

8.28.3.1. Caso se esgote o tempo para a solução da ocorrência, sem que seja sanado o defeito reclamado, a CONTRATADA deverá providenciar a substituição do equipamento ou módulo defeituoso;

8.28.3.2. O equipamento ou módulo utilizado na substituição deverá ser novo e original, recomendado pelo fabricante, com configuração igual ou superior ao substituído;

8.28.3.3. A substituição do equipamento ou módulo deverá ser em caráter definitivo e dentro do prazo máximo de 48 (quarenta e oito) horas úteis, contadas a partir da expiração do prazo de solução;

8.28.3.4. No caso de substituição do equipamento ou módulo, a CONTRATADA deverá entregar, em até 5 (cinco) dias úteis contados a partir da data da entrega, um documento onde constem as descrições e os números de série dos equipamentos ou módulos defeituosos utilizados na substituição;

8.28.3.5. Para fins de cálculo do período decorrido para solução da ocorrência de hardware, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência. Nos casos em que houver a substituição do equipamento ou módulo defeituoso para a solução da ocorrência, o seu fechamento efetivo se dará somente após a entrada em operação do novo equipamento ou módulo (de substituição), com todas as configurações necessárias ao seu pleno funcionamento.

8.28.4. Para os chamados de **Suporte Técnico referentes às ocorrências de software**, deverão ser considerados os seguintes prazos de acordo com os níveis de severidade:

Tabela 02

SUPORTE TÉCNICO PARA OCORRÊNCIAS DE SOFTWARE			
SEVERIDADE INFORMADA	**1º CONTATO COM A CONTRATANTE**	**TEMPO PARA SOLUÇÃO DE CONTORNO**	**TEMPO PARA SOLUÇÃO DEFINITIVA**
1	15 minutos	2 horas corridas	5 dias corridos

2	30 minutos	4 horas corridas	10 dias corridos
3	60 minutos	24 horas corridas	15 dias corridos
4	180 minutos	24 horas corridas	2 dias úteis
5	360 minutos	36 horas corridas	3 dias úteis

8.28.4.1. Considerando que as soluções das ocorrências de software, pela sua natureza, podem envolver atividades relacionadas ao desenvolvimento de patches específicos, admite-se, a adoção de solução de contorno (workaround) até que seja implementada a solução definitiva;

8.28.4.2. O tempo para a Solução de Contorno será contabilizado a partir do registro da ocorrência;

8.28.4.3. O tempo para a Solução Definitiva será contabilizado a partir do término do tempo para a disponibilização da Solução de Contorno;

8.28.4.4. Para fins de cálculo do período decorrido para solução da ocorrência de software, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência – seja essa solução de caráter definitivo ou provisório com a disponibilização de solução de contorno (workaround).

8.28.5. No atendimento dos chamados, para efeitos de apuração do tempo gasto pela CONTRATADA para a disponibilização da solução, serão desconsiderados os períodos em que a CONTRATANTE estiver responsável por executar ações necessárias para a análise e solução da ocorrência.

8.29. CENTRO DE SUPORTE E ASSISTÊNCIA TÉCNICA

8.29.1. No prazo máximo de 10 (dez) dias úteis, contados a partir do dia seguinte à assinatura do Contrato, a CONTRATADA deverá apresentar ao Conselho informações referentes ao centro de suporte e assistência técnica responsável pelo atendimento aos serviços de manutenção, se pertence ao fabricante dos produtos ou à própria CONTRATADA, endereço, telefone, e-mail e contato.

8.29.2. A CONTRATADA deverá providenciar o registro de toda e qualquer solicitação de manutenção e suporte técnico, independentemente de sua natureza, cabendo a CONTRATANTE, o devido acompanhamento.

8.29.2.1. À CONTRATANTE serão disponibilizados Website e telefone (0800) como canais de atendimento para abertura dos chamados, onde cada chamado deverá conter, no mínimo, o registro das informações abaixo:

8.29.2.1.1. Número do registro/ocorrência (a ser fornecido pela CONTRATADA);

8.29.2.1.2. Identificação do atendente;

8.29.2.1.3. Identificação do solicitante;

8.29.2.1.4. Data e hora da solicitação;

8.29.2.1.5. Nível de severidade da ocorrência (a ser fornecido pela CONTRATANTE);

8.29.2.1.6. Descrição da ocorrência;

8.29.3. No provimento deste serviço por meio de telefone, a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

8.29.4. Independente da forma que a CONTRATADA utilize para prestar os serviços de manutenção (por meio de Centro de Suporte e Assistência Técnica do fabricante dos produtos ou de centro de suporte e assistência técnica próprio), a mesma deverá permitir que a CONTRATANTE acompanhe, por meio de Website, o andamento de todos os chamados abertos por meio de telefone e de Website. Este acesso ao Centro de Suporte e Assistência Técnica deverá:

8.29.4.1. Estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, de segunda a domingo, incluindo os feriados;

8.29.4.2. Permitir realizar filtro por chamados encerrados em determinado intervalo de tempo, relacionados a um contrato específico;

8.29.4.3. Permitir realizar filtro por chamados com status “aberto”, com sua data de abertura no intervalo de tempo informado, relacionados a um contrato específico;

8.29.4.4. Permitir a apuração do tempo total de atendimento do chamado e o tempo em que o mesmo ficou sob a responsabilidade da CONTRATADA;

8.29.4.5. Exibir as informações do andamento dos chamados de forma completa, clara e precisa, permitindo identificar objetivamente as transições de responsabilidade entre CONTRATANTE e CONTRATADA pelas ações a serem realizadas;

8.29.4.6. Exibir as informações de data e hora de forma padronizada, incluindo o fuso horário a ser considerado.

8.29.5. O horário de abertura de chamado será determinado conforme abaixo:

8.29.5.1. Para chamados abertos pelo canal Telefone (0800), o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional da CONTRATANTE informando do problema ocorrido. Caso a atendente não possa informar o número de chamado neste momento, a mesma deverá, obrigatoriamente, informar um número de protocolo que registre a data e hora da ligação realizada.

8.29.5.2. Para chamados abertos pelo canal Website, o horário da abertura do chamado será a data e hora do registro do problema ocorrido. No momento do registro, a página web deverá informar o número de chamado.

8.29.6. O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA.

8.29.7. O serviço de registro de chamados deverá ser disponibilizado de acordo com a modalidade de atendimento estabelecida, remota ou presencialmente.

8.29.8. Não deverá haver qualquer limitação para o número de solicitações de suporte técnico remoto.

8.29.9. Não deverá haver qualquer limitação para o número de técnicos da CONTRATANTE autorizados a abrir chamados técnicos.

8.30. Durante o período de vigência contratual, a CONTRATADA deverá disponibilizar para a CONTRATANTE todas as atualizações dos softwares (atualização de versões, releases e patches), firmware ou microcódigos dos hardwares cobertos pela manutenção contratada, sem nenhum ônus adicional.

8.31. A CONTRATADA deverá notificar à CONTRATANTE sobre a liberação de novas versões e correções de software (patches) dos produtos cobertos pela manutenção contratada. Os avisos poderão ser encaminhados por e-mail, utilizando mecanismo automático de notificação.

8.32. Durante todo o período de prestação dos serviços relacionados ao objeto deste Termo de Referência, a CONTRATADA deverá apresentar, mensalmente, um arquivo contendo o registro de todas as ocorrências de suporte técnico do período mensal de prestação de serviços encerrado.

8.33. O Relatório Mensal de Atendimento deverá ser encaminhado para os Gestores Administrativo e Técnico em até 7 (sete) dias úteis, contados a partir do dia seguinte ao fim do período mensal de prestação de serviços e deverá estar no formato ".XLSX" (para ambiente MS Windows) ou outro formato definido em comum acordo.

8.34. O Relatório Mensal de Atendimento deverá conter as seguintes informações de cada ocorrência:

8.34.1.1. Número do registro/ocorrência;
8.34.1.2. Identificação do atendente;
8.34.1.3. Identificação do solicitante;
8.34.1.4. Data e hora da solicitação (considerando o fuso horário de Brasília);
8.34.1.5. Nível de severidade da ocorrência (estabelecido pela CONTRATANTE);
8.34.1.6. Descrição da ocorrência;
8.34.1.7. Data e hora da solução / fechamento da ocorrência (considerando o fuso horário de Brasília);
8.34.1.8. Identificação do responsável (CONTRATANTE) pelo fechamento;
8.34.1.9. Duração da ocorrência (no formato hh:mm);
8.34.1.10. Tempo de atendimento sob responsabilidade da CONTRATADA (no formato hh:mm);
8.34.1.11. Descrição detalhada da causa e da solução da ocorrência;
8.34.1.12. Informar se o chamado foi fechado com solução de contorno ou definitiva;
8.34.1.13. Informar o número do chamado original (quando o chamado for originário de outro onde se tiver feito uso da solução de contorno).

8.35. O atraso no envio do Relatório Mensal de Atendimento, implicará no atraso da análise técnica de suas informações. Tal análise serve de subsídio para a realização da medição do serviço prestado pela CONTRATADA no respectivo período e por conseguinte o faturamento do mesmo.

9. IMPLANTAÇÃO PARA A EXECUÇÃO DOS SERVIÇOS

9.1. A CONTRATADA deverá implantar todos os componentes da solução objeto deste contrato, no prazo máximo de 80 (oitenta) dias corridos, após a assinatura do Contrato.

9.2. O prazo estipulado de 80 (oitenta) dias corridos contempla as atividades destacadas conforme o cronograma estabelecido a seguir:

9.2.1. A partir da assinatura do contrato, a CONTRATADA deverá cumprir com os seguintes prazos:

9.2.1.1. FASE 01 – Planejamento e Levantamento de Informações, 15 (quinze) dias corridos;

9.2.1.2. FASE 02 – Entrega das Soluções utilizadas na prestação do serviço, 60 (sessenta) dias corridos;

9.2.1.3. FASE 03 – Implantação, migração de regras e configurações existentes, 15 (quinze) dias corridos;

9.2.1.4. FASE 04 – Entrega da documentação, 02 (dois) dias corridos;

9.2.1.5. As fases poderão ocorrer em paralelo de modo a acelerar o processo de implantação do ferramental necessário à execução dos serviços;

9.2.1.6. Cada fase e suas atividades principais são descritas posteriormente neste documento;

9.2.1.7. Os prazos poderão ser dilatados mediante eventos extraordinários que sejam comprovados pela CONTRATADA e caso a CONTRATANTE esteja de acordo com os mesmos;

9.2.2. Atrasos dentro dos prazos de entrega:

9.2.2.1. Comete infração administrativa a CONTRATADA que:

9.2.2.2. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

9.2.2.3. Ensejar o retardamento da execução do objeto;

9.2.2.4. Fraudar na execução do contrato;

9.2.2.5. Comportar-se de modo inidôneo;

9.2.2.6. Cometer fraude fiscal;

9.2.2.7. Não mantiver a proposta.

9.2.2.8. Ao término dos 80 dias, contados a partir da assinatura do Contrato, poderá ser aplicada multa moratória de 0,50% (cinquenta centésimos por cento), em cima do valor global do contrato, por dia de atraso;

9.2.2.9. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo máximo de 20 (vinte) dias, a contar da notificação da CONTRATANTE, sem qualquer prejuízo ao CN-SESI e com possibilidade de aplicação de penalidades;

9.3. A implantação da solução deverá ser realizada por um profissional qualificado com certificação oficial na solução sendo nível Engenheiro ou Implementador.

9.4. Para o fornecimento e instalação dos equipamentos, a CONTRATADA deverá observar o seguinte:

9.4.1. Fornecer todos os cabos de ligação lógica e os componentes elétricos necessários à instalação e funcionamento;

9.4.2. Fornecer todos os equipamentos e softwares conforme as características e especificações técnicas mínimas;

9.4.3. Todos os itens deverão implementar todas as características descritas nas especificações técnicas;
9.4.4. Deverão ser fornecidos todos os documentos e manuais necessários para garantir o bom funcionamento, suporte e manutenção dos itens fornecidos;

9.5. Não serão aceitos softwares “beta” ou em desenvolvimento.

9.6. A CONTRATADA deverá elaborar projeto contendo:

9.6.1. Layout do conjunto a ser adquirido informando os modelos e a quantidade de cada item, e como serão logicamente interconectados;
9.6.2. Instalar e configurar todos os equipamentos a serem fornecidos, incluindo toda a documentação com a descrição do processo de instalação e configuração.
9.6.3. São atividades inerentes à instalação e configuração, as quais devem ser executadas pela CONTRATADA:
9.6.3.1. Elaboração da documentação, contendo no mínimo os seguintes itens:
9.6.3.2. Cronograma;
9.6.3.3. Levantamento de informações sobre o ambiente atual;
9.6.3.4. Definição dos parâmetros de configuração básicos e avançados a serem implementados;
9.6.3.5. Mapa de rede contendo a topologia a ser implementada ou atualizada;
9.6.3.6. Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;
9.6.3.7. Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.
9.6.3.8. Configuração em cluster modalidade ativo/passivo.
9.6.3.9. Otimização das regras e objetos de segurança da solução implantada, objetivando a redução do número de políticas de segurança e ganhos de desempenho.
9.6.3.10. Integração com a ferramenta de correlação de eventos, caso exista, para coleta, monitoramento e correlação de registros de segurança da informação.
9.6.3.11. Integração com ferramenta de monitoramento via SNMP, caso exista.

9.7. A implementação da infraestrutura proposta deverá efetuar o aproveitamento máximo dos produtos (hardwares e softwares) existentes na CONTRATADA e manter o ambiente de rede atual em produção;
9.8. O ambiente proposto deverá ser criado em módulos e definindo-se uma ordem sequencial para sua implantação à qual denominamos fases;

9.9. **FASE 01 – Planejamento e Levantamento de informações;**

9.9.1. Todos os passos desta fase deverão ser documentados, assim como os problemas encontrados e suas soluções;
9.9.2. A empresa deverá realizar reuniões de planejamento e consultoria com a CONTRATANTE a fim de definir os detalhes técnicos requeridos para as configurações contratadas;

9.9.3. A CONTRATADA consolidará o detalhamento das especificações necessárias para a implementação dos serviços, gerando assim o documento de Plano de Configuração e Integração, que será entregue à CONTRATANTE;
9.9.4. A CONTRATADA também deverá preparar e fornecer o documento Plano de Homologação e Testes contendo os testes que serão executados para validar a solução implementada;
9.9.5. Para o detalhamento técnico, a empresa deverá colocar à disposição da CONTRATANTE técnicos especializados nas tecnologias dos serviços contratados;
9.9.6. Nesta fase serão definidas ao menos as seguintes atividades:
9.9.6.1. Levantamento de toda infraestrutura afeta à solução: produtos de hardware, software, cabeamento, licenças e demais informações;
9.9.6.2. Consultoria para implementar o serviço de acordo com as melhores práticas do fabricante da solução ofertada;
9.9.6.3. Planejamento da implementação da solução;
9.9.6.4. Desenho da arquitetura lógica da solução, contendo a topologia da solução, indicando as alterações com relação à topologia atual;
9.9.6.5. Desenho da arquitetura física da solução, contendo tabela de conectividade física da solução, com o mapeamento das conexões necessárias diretamente nos dispositivos de rede da CONTRATANTE;
9.9.6.6. Preparação do documento com detalhes da implementação da solução, contemplando no mínimo o planejamento detalhado das ações necessárias para implantação da nova solução;
9.9.6.7. Preparação do documento com detalhes de contingenciamento de recursos e serviços da solução – Plano de Contingência, descrevendo as ações necessárias para restabelecimento do ambiente à normalidade, no evento de falhas no funcionamento da nova solução que causem interrupção no fluxo de dados da rede da CONTRATANTE;
9.9.6.8. Preparação dos procedimentos de testes para validação da solução – Plano de Homologação e Testes;
9.9.6.9. E, ainda, qualquer documento técnico que seja necessário para atender aos requerimentos constantes;
9.9.7. Entregas previstas para a fase:
9.9.7.1. Escopo da Solução;
9.9.7.2. Identificação de todos os ativos;
9.9.7.3. Desenho da arquitetura lógica da solução;
9.9.7.4. Desenho da arquitetura física da solução;
9.9.7.5. Plano de Configuração e Integração;
9.9.7.6. Plano de Homologação e Testes;
9.9.7.7. Documentos de acompanhamento do projeto, incluindo relatórios de situação e atas de reunião;

9.10. **FASE 02 – Entrega das Soluções utilizadas na prestação do serviço;**

9.10.1. Os equipamentos, as mídias e os softwares deverão ser entregues na CTIC da CONTRATANTE, situada no Edifício Armando Monteiro Neto SBN Quadra 01, Bloco I, 6º andar, Brasília - DF,

70040-913, em dias úteis, durante o horário de 08:00 às 12:00 e de 14:00 às 18:00hs;
9.10.2. Os equipamentos deverão ser entregues acondicionados adequadamente, de forma a permitir completa segurança durante o transporte;
9.10.3. Quando for o caso, os volumes contendo os equipamentos deverão estar identificados externamente com os dados constantes da nota fiscal, fatura e o endereço de entrega;
9.10.4. Em casos de equipamentos importados, deverá ser entregue a comprovação da origem dos bens importados e comprovação da quitação dos tributos de importação a eles referentes, conforme Decreto nº 7.174/2010;

9.11. **FASE 03 – Implantação, migração de regras e configurações existentes;**

9.11.1. A Solução deverá ser instalada e configurada no Datacenter da CONTRATANTE, Edifício Armando Monteiro Neto SBN Quadra 01, Bloco I, 6º e 7º andares, Brasília - DF, 70040-913;
9.11.2. Todos os passos desta fase deverão ser documentados, assim como os problemas encontrados e suas soluções;
9.11.3. A instalação/configuração deverá ser realizada de tal forma que as interrupções no ambiente de Produção sejam as mínimas possíveis e estritamente necessárias e, ainda, não causem transtornos aos usuários finais da CONTRATANTE;
9.11.4. A Contratada deverá executar uma série de testes funcionais básicos para verificar o perfeito funcionamento do ambiente;
9.11.5. É de responsabilidade da Contratada a instalação de todos os produtos, sejam estes de hardware e/ou software;
9.11.6. Deverão ser fornecidos pela Contratada, quando da instalação dos produtos, todos os cabos, conectores e acessórios (todos os elementos passivos) necessários e para a montagem apropriada dos equipamentos nos locais indicados;
9.11.7. Os testes e validações deveram ser documentados e os erros encontrados apresentados a CONTRATANTE e a forma de solução utilizada;

9.12. **FASE 04 – Entrega da documentação;**

9.12.1. A empresa deverá consolidar toda a “Documentação do Projeto” e entregá-la em mídia eletrônica no encerramento do “Cronograma de Execução” e/ou do projeto;
9.12.2. Fazem parte da Documentação do Projeto:
9.12.2.1. Todos os documentos técnicos gerados durante o projeto;
9.12.2.2. Todos os documentos de controle e gerência da execução do Contrato;
9.12.2.3. Todos os documentos mencionados neste Termo de Referência;
9.12.3. A CONTRATADA deverá conduzir uma reunião formal com a CONTRATANTE, para:
9.12.3.1. Entregar a “Documentação do Projeto”;
9.12.3.2. Releitura das atividades e produtos definidos no Escopo e concluídos pela Contratada;
9.12.3.3. Releitura das questões de suporte e obrigações entre as partes;

9.12.3.4. Obter a assinatura do Relatório Final do Projeto indicando o encerramento do projeto e do Termo de Aceitação do Objeto.

9.13. Estes serviços deverão ser realizados por profissionais experientes, especialistas e certificados nos produtos ofertados;

10. GARANTIAS

10.1. Todos os componentes de software e/ou firmware, bem como todas as funcionalidades requisitadas, do serviço a ser prestado deverão estar habilitados pela vigência completa da prestação do serviço, bem como deverão perdurar por, no mínimo, 12 (doze) meses após o término do contrato, de modo a respaldar o conselho em uma eventual readequação para a execução de novos serviços de TIC;

10.2. Licenças com direito de atualização dos softwares envolvidos na solução quando:

10.2.1. Novas versões, revisões, distribuições (release), correções (patches) dos programas e assinaturas forem disponibilizadas;
10.2.2. Houver lançamento de novos softwares em substituição aos fornecidos;
10.2.3. Ficar caracterizada descontinuidade dos softwares fornecidos;

10.3. Deve ser fornecida garantia de atualização e subscrição de assinatura de ataques e ameaças, para o período de validade do contrato, capaz de ativar regularmente novas assinaturas de ataques e ameaças, atualizadas e mantidas pela equipe do fabricante, através de pesquisa e monitoramento 24x7 da Internet;

10.4. Deve ser fornecida garantia de reposição de hardware, para o período de validade do contrato, de forma a cobrir situações em que sejam identificados problemas nos hardwares da solução ofertada.

11. QUALIFICAÇÃO TÉCNICA

11.1. Comprovações técnicas necessárias:

11.1.1. Ao menos um atestado de bom desempenho anterior (Capacidade Técnica) relativo à prestação de serviço de SOC de mesma natureza da presente licitação, expedido por pessoa jurídica de direito público ou privado que comprove(m) aptidão para o desempenho do serviço licitado.
11.1.2. Ao menos um atestado de bom desempenho anterior (Capacidade Técnica) relativo à solução de Next Generation Firewall de mesma natureza da presente licitação, expedido por pessoa jurídica de direito público ou privado que comprove(m) aptidão para o desempenho do serviço licitado.
11.1.3. A CONTRATADA deverá ter ao menos 2 (dois) profissionais empregados e qualificados de acordo com as certificações das soluções de perímetro empregadas na prestação dos serviços;

11.1.3.1. Não serão aceitas certificações de vendas, nem de parcerias;

11.1.4. O SOC deverá contar com profissionais capacitados para a realização das atividades de monitoramento de segurança, contendo, no mínimo, um profissional com os certificados válidos para, pelo menos, duas das competências abaixo:

11.1.4.1. ISO/IEC 27001, ISO/IEC 27002 ou similar;

11.1.4.2. Operação e administração da Solução de Prevenção de Ameaças de próxima geração da solução ofertada com o nível de engenheiro/administrador;

11.1.4.3. Resposta a Incidentes de Segurança;

11.1.5. A CONTRATADA deverá possuir, na data de início da prestação dos serviços, recursos operacionais e profissional(is) que detenham as certificações do fabricante da solução ofertada com comprovada regularidade para desempenho de atividades pertinentes e compatíveis com o objeto do Termo de Referência. A comprovação deverá ser por meio de Declaração firmada pelo representante legal da licitante.

11.1.5.1. O(s) Profissional(is) deverá(ão) pertencer ao quadro da CONTRATADA, entendendo-se como tal, para fins do Termo de Referência, o sócio que comprove seu vínculo por intermédio de Contrato/Estatuto Social; o Administrador ou o Diretor; o empregado devidamente registrado em Carteira de Trabalho e Previdência Social ou ainda a comprovação da disponibilidade do profissional mediante contrato de prestação de serviços, sem vínculo trabalhista e regido pela legislação civil.

12. SIGILO E INVIOLABILIDADE

12.1. A CONTRATADA deverá assinar TERMO DE CONFIDENCIALIDADE E SIGILO – ANEXO I, a fim de garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante a prestação dos serviços de suporte técnico.

12.2. A **CONTRATADA** deverá prestar esclarecimentos à **CONTRATANTE** sobre eventuais atos ou fatos noticiados que se refiram à mesma.

13. SANÇÕES ADMINISTRATIVAS

13.1. Será aplicada multa pelo descumprimento dos prazos relacionados no **item 8 – NÍVEIS DE ACORDO DE SERVIÇO** deste **Termo de Referência**, causado pela **CONTRATADA**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

13.2. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

13.2.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,1% (um décimo por cento) ao dia do valor total do respectivo Contrato;

13.2.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea “13.2.1” será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total do respectivo Contrato.

13.3. Será aplicada multa pelo atraso, causado pela **CONTRATADA**, no **fornecimento das informações sobre os canais de atendimento**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

13.4. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

13.4.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,05% (cinco centésimos por cento) ao dia do valor total do respectivo Contrato;
13.4.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea "13.4.1" será substituída por multa de 0,1% (um décimo por cento) ao dia, até o limite máximo de 2% (dois por cento) do valor total do respectivo Contrato.

13.5. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 0,1% (um décimo por cento) à hora, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela **CONTRATADA,** no **cumprimento dos prazos para solução das ocorrências,** causado pela **CONTRATADA**, **para cada chamado registrado pela CONTRATANTE**. O descumprimento de mais de um prazo para um mesmo chamado implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

13.6. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela **CONTRATADA**, **no fornecimento da solução definitiva para as ocorrências de *software***. O descumprimento do prazo de cada chamado registrado pela **CONTRATANTE** implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

13.7. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de até 5% (cinco por cento), pelo atraso, causado pela **CONTRATADA**, **no fornecimento de qualquer um dos relatórios solicitados**, deste **Termo de Referência**.

13.8. Será aplicada multa de 0,25% (vinte e cinco centésimos por cento) à 10% (dez por cento) do valor total do respectivo Contrato **pelo inadimplemento contratual relacionado às situações não previstas nos subitens anteriores.**

13.9. As multas constantes nesse item poderão ser aplicadas cumulativamente conforme o caso e são meramente moratórias, não isentando a **CONTRATADA** o ressarcimento por perdas e danos pelos prejuízos a que der causa.

13.10. Caso o valor total pago mensalmente pela CONTRATANTE para manutenção dos equipamentos seja insuficiente para o débito das multas devidas pela **CONTRATADA** no referido mês, o valor devido deverá ser descontado **integralmente** do valor caucionado em garantia do cumprimento das obrigações contratuais.

13.11. À **CONTRATADA** será garantido o direito à apresentação de defesa prévia nos moldes da legislação vigente.

14. OBRIGAÇÕES DA CONTRATADA

14.1. Em **até 20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Contrato, a **CONTRATADA** deverá encaminhar antes da data de início da realização dos serviços, relação nominal dos empregados que atuarão no serviço, indicando o CPF e a área de atuação juntamente com a documentação comprobatória da qualificação para prestação do serviço contratado de acordo com o especificado neste termo de referência;

14.2. Manter os empregados devidamente identificados por meio de crachá da empresa, quando em trabalho nas dependências da CONTRATANTE;

14.3. Promover treinamento e atualização dos empregados que prestam serviços para a CONTRATANTE, de acordo com as necessidades do serviço e sempre que o fiscalizador do contrato entender conveniente à adequada execução dos serviços contratados;

14.4. Responsabilizar-se pelo transporte do seu pessoal até o Conselho Nacional do SESI sempre que necessário, sem custo para a CONTRATANTE, inclusive em casos de paralisação dos transportes coletivos, bem como nas situações nas quais se faça necessária a execução dos serviços em regime extraordinário;

14.5. Cuidar para que todos os privilégios de acesso a sistemas, informações e recursos da CONTRATANTE sejam revistos, modificados ou revogados quando da transferência, remanejamento, promoção ou demissão de profissionais sob sua responsabilidade;

14.6. Remeter tempestivamente a CONTRATANTE lista atualizada dos empregados envolvidos na prestação dos serviços contratados, sempre que houver substituição, indicando o CPF e a área de atuação juntamente com a documentação comprobatória da qualificação para prestação dos serviços contratados;

14.7. Encaminhar à unidade fiscalizadora da CONTRATANTE todas as faturas dos serviços prestados;

14.8. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes desta contratação;

14.9. Responder por quaisquer danos causados diretamente a bens de propriedade da CONTRATANTE ou de terceiros, quando tenham sido causados por seus empregados e/ou prepostos durante a execução dos serviços contratados;

14.10. Participar, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reunião de alinhamento de expectativas contratuais com equipe da CONTRATANTE;

14.11. Manter-se, durante o período de vigência do contrato, em conformidade com as obrigações trabalhistas, todas as condições de habilitação e qualificação exigidas na licitação;

14.12. Planejar, desenvolver, implantar, executar e manter os serviços objetos do contrato dentro dos acordos de níveis de serviços estabelecidos;

14.13. Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com a CONTRATANTE;

14.14. Obedecer rigorosamente às normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação da CONTRATANTE;

14.15. A CONTRATADA obriga-se a não empregar menores de 18 anos em trabalho noturno, perigoso ou insalubre, bem como a não empregar menores de 16 anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos.

14.16. Se for necessário, e a critério da CONTRATANTE, poderá ser solicitada a execução dos serviços em dias e horários distintos dos estabelecidos, desde que a necessidade seja acordada previamente com a CONTRATADA;

14.17. Deverá fornecer todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a, um kit de fixação para rack, trilhos para montagem do tipo retrátil, permitindo o deslizamento dos equipamentos a fim de facilitar sua manutenção, cabos de alimentação elétrica, além de todas as licenças de softwares necessárias para o funcionamento da solução conforme requisitos mínimos deste termo de referência;

14.18. Todos os equipamentos e acessórios deverão ser entregues novos e de primeiro uso, acondicionados em suas embalagens originais;
14.19. É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da CONTRATANTE; e

14.20. É vedada a subcontratação de outra empresa para a execução dos serviços, objeto desta contratação.

15. OBRIGAÇÕES DA CONTRATANTE

15.1. Fiscalizar e acompanhar a prestação do serviço/objeto contratual, comunicando à CONTRATADA toda e qualquer deficiência e/ou irregularidade relacionada com os serviços de manutenção do objeto, diligenciando nos casos que exigirem providências corretivas.
15.2. Permitir acesso dos empregados da CONTRATADA às suas dependências, equipamentos, softwares e sistemas para a execução dos serviços;

15.3. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da CONTRATADA ou por seus prepostos;

15.4. Avaliar e homologar relatório mensal dos serviços executados pela CONTRATADA, observando os indicadores e metas de níveis de serviço, conforme descrito neste Termo de Referência e nas suas partes;

15.5. Efetuar os pagamentos devidos pela execução dos serviços, desde que cumpridas todas as formalidades e exigências do contrato;

15.6. Exercer a fiscalização dos serviços prestados, por meio de pessoal designado;

15.7. Comunicar oficialmente à CONTRATADA qualquer falha verificada no cumprimento do contrato.

16. VIGÊNCIA

16.1. O prazo para a prestação de serviço deverá ser pelo período de 12 (doze) meses, a contar da data da assinatura, admitida a sua prorrogação, condicionada à prévia e expressa anuência das partes, formalizada mediante termo aditivo, até o limite de 60 (sessenta) meses previsto no parágrafo único do art. 26 do Regulamento de Licitações e Contratos do SESI.

17. RESCISÃO

17.1. Pelo descumprimento de quaisquer de suas cláusulas e condições, poderá o CN-SESI rescindir o presente contrato, independentemente de prévia interpelação judicial, respondendo a CONTRATADA pelos prejuízos ocasionados, ressalvadas as hipóteses de caso fortuito ou força maior, desde que devidamente comprovados.

18. FISCALIZAÇÃO DOS SERVIÇOS

18.1. A área técnica responsável da CONTRATANTE fiscalizará os serviços realizados pela CONTRATADA e, poderá, a qualquer tempo, solicitar um relatório detalhado sobre os serviços prestados – pontualmente ou mensalmente, sejam eles de qualquer natureza, de modo a validar os valores para fins de aprovação do pagamento.

19. FORMA DE PAGAMENTO

19.1. O pagamento deverá ser realizado em até 30 (trinta) dias, contados da medição mensal dos serviços, mediante a apresentação da Nota Fiscal/Fatura devidamente aprovada pelo Gestor do Contrato.

19.1.1. O início do pagamento previsto no subitem anterior se dará após a implementação e o pleno funcionamento da solução de SOC.

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N° 02/2021
SESI – CONSELHO NACIONAL

ANEXO I (A) – TERMO DE CONFIDENCIALIDADE E SIGILO

A empresa _____ _____[RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em _____[ENDEREÇO], inscrita no CNPJ/MF com o n.º _____ [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações produzidas ou custodiadas do Conselho Nacional do SESI – CN-SESI, incluindo sobre o ambiente computacional corporativo, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações sensíveis, incluindo as de propriedade exclusiva do CN-SESI reveladas à EMPRESA RECEPTORA em função da vistoria prévia realizada para atendimento ao edital do Pregão nº _____ [N.º DO PREGÃO].

3. A expressão "informação sensível" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CN-SESI, das informações sensíveis reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CN-SESI, as informações sensíveis reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento às pessoas estritamente necessárias que estejam diretamente envolvidas nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CN-SESI, devendo cientificá-las da existência deste Termo e da sensibilidade das informações reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.
8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CN-SESI qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações reveladas, devidamente comprovada, sem autorização expressa do CN-SESI, por ação ou omissão da EMPRESA RECEPTORA, em especial qualquer divulgação, utilização, transferência, cessão ou alienação, intencional ou não de qualquer informação confidencial, material, documentos e informações ao mercado e/ou a outras pessoas físicas e jurídicas, ensejará sanções, pagamento ou recomposição sobre perdas e danos sofridos pelo CN-SESI, inclusive sobre as de ordem moral, sem prejuízo da responsabilização civil, criminal e administrativa, as quais serão apuradas em regular processo judicial/administrativo, na forma da lei, assegurados o contraditório e a ampla defesa.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CN-SESI.

E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo por meio de seus representantes legais.

Brasília-DF, ___ de _____ de 202_.

_____
[NOME DA EMPRESA RECEPTORA]

_____
(Nome, CPF e função do preposto da empresa RECEPTORA)

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N° 02/2021
SESI – CONSELHO NACIONAL

ANEXO I (B) -- ATESTADO (OU DECLARAÇÃO) DE CAPACIDADE TÉCNICA

Atestamos (ou declaramos) que a empresa _____, inscrita no CNPJ (MF) nº _____,inscrição estadual nº _____, estabelecida no (a) _____, executa (ou executou) serviços de _____ para esta empresa (ou órgão).

Atestamos (ou declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Local e data

_____
Assinatura e carimbo do emissor

Observações:
1) Este atestado (ou declaração) deverá ser emitido em papel que identifique o órgão (ou empresa) emissor; e
2) o atestado (ou declaração) deverá estar visado pelo respectivo órgão fiscalizador, quando for o caso.

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N° 02/2021
SESI – CONSELHO NACIONAL

ANEXO II – FORMULÁRIO DE PROPOSTA DE PREÇOS

LICITANTE: TELEFONE DE CONTATO:		
END. COMERCIAL: CIDADE:	UF:	CEP:
FONE:	FAX:	E-MAIL:
CNPJ:	INSCRIÇÃO ESTADUAL:	
DATA: VALIDADE DA PROPOSTA: DADOS BANCÁRIOS: DADOS DO REPRESENTANTE DA EMPRESA:		

ITEM	DESCRIÇÃO DO SERVIÇO	QUANT.	UND.	VALOR MENSAL	VALOR TOTAL
1	Serviços Gerenciados de Segurança	12	MÊS		
				VALOR TOTAL DA PROPOSTA	**R$**

VALOR GLOBAL TOTAL DA PROPOSTA EM R$ ..... (POR EXTENSO)

A validade desta proposta é de **60 (sessenta) dias corridos**, contados da data da abertura da sessão pública de **PREGÃO ELETRÔNICO**.

A apresentação da proposta implicará na plena aceitação das condições estabelecidas neste edital e seus anexos.

....., ..., ... de 2021.
Local e Data

Assinatura do Responsável pela Empresa
(Nome Legível/Cargo)

***Juntamente com a proposta definitiva o licitante deverá encaminhar, quando solicitado, o disposto no subitem 14.11 do edital.**

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO N° 02/2021
SESI – CONSELHO NACIONAL

ANEXO III – MINUTA DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS

MINUTA DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS Nº XXXX QUE, ENTRE SI, CELEBRAM O SERVIÇO SOCIAL DA INDÚSTRIA - CONSELHO NACIONAL – SESI/CN E A EMPRESA XXXXXXXXXX, NA FORMA ABAIXO:

O **SERVIÇO SOCIAL DA INDÚSTRIA (SESI) - CONSELHO NACIONAL**, com sede no Setor Bancário Norte (SBN), Quadra 01, lote 28, Bloco I, 6º e 7º andares, no Edifício Armando Monteiro Neto, Brasília - DF, inscrito no CNPJ 03.800.479/0001-39, neste ato representado por seu Superintendente Executivo, **PEDRO ANTÔNIO FIORAVANTE SILVESTRE NETO,** brasileiro, casado, portador do RG nº 020.936.982-6 expedido pelo MD/EB e inscrito no CPF sob o nº 498.981.087-20, doravante denominado **CONTRATANTE**, e, de outro lado, a empresa XXXXXXXXXX, inscrita no CNPJ/MF sob o n. 000000000, com sede na xxxxxxxxxxxxxxxxxx, CEP: 0000000, representada neste ato por seu Procurador, o Sr. XXXXXXXXXXXXXXX, [nacionalidade], [estado civil], portador do RG n. 0000000000 SSP/DF, e inscrito no CPF/MF sob o nº 0000000000, residente e domiciliado nessa capital, doravante denominada **CONTRATADA**, têm entre si, justo e avençado o presente Contrato de Prestação de Serviços, o qual se regerá pelos termos do Edital de **Pregão Eletrônico nº 02/2021**, constante nos autos do **Processo SESI/CN nº 0117/2020**, realizado com base no Regulamento de Licitações e Contratos do SESI, DOU de 16/09/1998, com as posteriores alterações publicadas em 26/10/2001, 11/11/2002, 24/02/2006, 11/05/2011 e 23/12/2011, além da proposta apresentada no mencionado certame, pelas cláusulas e condições especificadas a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Fornecimento de Solução Integrada de Serviços Gerenciados de Segurança que contemplem serviços de segurança de perímetro com fornecimento de equipamentos, administração e monitoração de segurança, resposta a incidentes de segurança e transferência de conhecimento para a equipe técnica do Conselho Nacional do SESI, conforme especificações, quantitativos e demais condições estabelecidas nos autos do processo administrativo em epígrafe, no edital de licitação e de acordo com as normas e condições definidas neste instrumento contratual.

CLÁUSULA SEGUNDA – DAS OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

2.1. As obrigações do CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

CLÁUSULA TERCEIRA – DA SUBCONTRATAÇÃO
3.1. Não será admitida a subcontratação do objeto licitatório.

CLÁUSULA QUARTA – DA INEXISTÊNCIA DE VÍNCULO DE EMPREGO

4.1. O presente contrato não gera qualquer vínculo de emprego entre o SESI/CN e os eventuais prestadores alocados pela CONTRATADA, na execução dos serviços objeto deste contrato, não existindo obrigação de horário e subordinação técnica ou administrativa ao SESI/CN, com o que desde já consente a CONTRATADA, que assumirá qualquer responsabilidade que eventualmente venha a ser imposta a esta entidade.

CLÁUSULA QUINTA – DA GESTÃO E DA FISCALIZAÇÃO

5.1. A CONTRATADA obriga-se a fornecer ao SESI/CN, ou preposto seu, toda e qualquer informação que lhe seja solicitada sobre o objeto deste contrato, bem como facilitar a fiscalização do objeto contratual.

5.2. Caberá ao SESI/CN, por meio do gestor e fiscal do presente contrato, empregados indicados e designados pela Superintendência, por ato específico para este fim, o acompanhamento, a fiscalização e a avaliação do objeto deste contrato, exigindo da CONTRATADA o cumprimento das disposições contidas neste instrumento e exercendo a aferição qualitativa e quantitativa do objeto contratual em estrita observância ao normativo interno que trata sobre a gestão das contratações da entidade.

5.3. O exercício da fiscalização pelo SESI/CN não elide nem diminui a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade ou resultante de imperfeições técnicas ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implicará em corresponsabilidade do SESI/CN.

5.4. A qualquer tempo, o SESI/CN poderá solicitar a substituição de qualquer membro da equipe técnica da CONTRATADA que venha a prejudicar, conforme o critério do fiscal do contrato, o bom andamento dos serviços.

5.5. O SESI/CN não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, técnicos, dentre outros.

5.6. O SESI/CN será reservado o direito de rejeitar, no todo ou em parte, os serviços prestados em desacordo com o contrato, devendo a CONTRATADA refazer ou substituir as partes que apresentem defeitos, sem ônus adicionais a esta entidade.

5.7. Os representantes do SESI/CN reportar-se-ão diretamente aos profissionais da CONTRATADA.

5.8. Os representantes do SESI/CN fiscalizarão os serviços realizados pela CONTRATADA e, poderá, a qualquer tempo, solicitar um relatório detalhado sobre os serviços prestados – pontualmente ou mensalmente, sejam eles de qualquer natureza –, de modo a validar os valores para fins de aprovação do pagamento.

CLÁUSULA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

6.1. As despesas com o objeto deste contrato correrão por conta dos recursos previstos no orçamento anual do SESI/CN, ficando a discriminação do código orçamentário específico vinculado ao projeto para o qual sejam demandadas as ações, podendo ser aumentado de acordo com a necessidade.

CLÁUSULA SÉTIMA – DA VIGÊNCIA

7.1. Este contrato terá a vigência de 12 (doze) meses, a contar da data da assinatura, admitida a sua prorrogação, condicionada à prévia e expressa anuência das partes, formalizada mediante termo aditivo, até o limite de 60 (sessenta) meses previsto no parágrafo único do art. 26 do Regulamento de Licitações e Contratos do SESI.

CLÁUSULA OITAVA – DO PREÇO

8.1. O SESI/CN pagará à CONTRATADA o preço total de **R$ XXXXXXXX,XX (xxxxxxxxxxxxxxx),** constante na homologação e faturado conforme demanda do SESI/CN, respeitando-se, para tanto, as especificações e valores descritos abaixo:

ITEM	DESCRIÇÃO DO SERVIÇO	QUANT.	UND.	VALOR MENSAL	VALOR TOTAL
1	Serviços Gerenciados de Segurança	12	MÊS		
				VALOR TOTAL DA PROPOSTA	**R$**

8.2. O valor acima abrange as despesas necessárias à boa execução do objeto contratual.

8.3. Os valores inicialmente contratados serão fixos e irreajustáveis pelo tempo de vigência do presente contrato. Entretanto, poderão ser reajustados, em caso de renovação contratual, pela variação do IGP-M no período.

8.4. Na hipótese de renovação contratual, os pedidos de reajuste deverão ser feitos antes de assinado o respectivo Termo Aditivo e requerida a ressalva neste sentido, pela CONTRATADA, no

bojo do documento em que esta se manifesta pelo interesse da prorrogação contratual, sob pena de preclusão lógica deste direito.

8.5. Os serviços ora contratados serão demandados conforme interesse e conveniência do SESI/CN. Assim, esta entidade não está obrigada a requerer o valor total contratado. Por conseguinte, a CONTRATADA, não apenas está ciente das condições contratuais ora descritas, como também com elas concorda.

8.6. Todos os impostos, taxas, seguros já deverão estar inclusos no valor apresentado pela CONTRATADA.

CLÁUSULA NONA – DA FORMA DE PAGAMENTO

9.1. A nota fiscal/fatura, contendo o detalhamento dos serviços executados, deverá ser entregue ao Conselho Nacional do SESI, após o recebimento do serviço pelo contratante.

9.1.1. A empresa Contratada deverá apresentar nota fiscal, acompanhada da seguinte documentação: CNPJ; Prova de Inscrição no Cadastro de Contribuintes Estadual e Municipal – compatível com o objeto social; CR/FGTS; CERTIDÃO DE QUITAÇÃO DE TRIBUTOS E CONTRIBUIÇÕES FEDERAIS, INCLUINDO AS CONTRIBUIÇÕES SOCIAIS; CERTIDÃO DE REGULARIDADE DO GDF, para as empresas sediadas em Brasília; e, CERTIDÃO DE REGULARIDADE ESTADUAL E MUNICIPAL, para as empresas sediadas em outras localidades deste Edital, para liquidação e pagamento da despesa contraída pela entidade que compõem o SESI.

9.2. O pagamento deverá ser realizado em até 30 (trinta) dias, contados da medição mensal dos serviços, mediante a apresentação da Nota Fiscal/Fatura devidamente aprovada pelo Gestor do Contrato.

9.2.2. O início do pagamento previsto no subitem anterior se dará após a implementação e o pleno funcionamento da solução de SOC.

9.3. O pagamento será efetuado em até 10 (dez) dias após o recebimento da Nota Fiscal, contendo o "atesto" pelo recebimento dos serviços pelo Fiscal do contrato.

9.4. Havendo erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o Conselho Nacional do SESI.

9.5. O pagamento será creditado em favor da Contratada por meio de ordem de pagamento bancária, devendo, para isto, ficar explicitado o nome, número da agência e o número da conta corrente.

9.6. A empresa Contratada estará sujeita às retenções tributárias legais, devendo ser informado no corpo da Nota Fiscal as deduções às quais ela se adequa.

9.7. A Contratada optante pelo SIMPLES NACIONAL deverá enviar junto com a nota fiscal, a declaração de optante pelo SIMPLES NACIONAL com indicação da Lei regulamentadora.

9.8. O preenchimento da nota fiscal deverá ser conforme orientação da fiscalização, devendo a mesma conter também as informações dos tributos a serem descontados, tais como: INSS, IRPJ, CSSLL, CONFINS, PIS e ISS, quando houver.

9.9. A Nota Fiscal/Fatura, para liquidação e pagamento dos materiais e ferramentas, deverá estar obrigatoriamente atestada pela área demandante, bem como acompanhada da documentação exigida, dentro do prazo de validade.

9.10. Em hipótese alguma será efetuado pagamento por meio de boleto bancário.

9.11. Para liquidação dos valores relativos à Prestação de Serviços objeto deste Edital, o SESI/CN assegura-se o direito:

9.11.1. Recusar o pagamento caso a Prestação de Serviços do objeto não seja realizado de acordo com o proposto, aceito e pactuado.

9.11.2. Deduzir do montante a pagar as indenizações devidas pela empresa Contratada em razão da inadimplência nos termos do Contrato que vier a ser firmado.

9.11.3. Devolver à Contratada as Notas Fiscais não aprovadas para as devidas correções, acompanhadas dos motivos de sua rejeição, recontando-se para pagamento o prazo 10 (dez) dias após o recebimento da Nota Fiscal, a partir da sua reapresentação, sem qualquer tipo de correção de seu valor, sendo automaticamente alteradas as datas de vencimento, não respondendo os proponentes do SESI/CN por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

CLÁUSULA DÉCIMA – GARANTIA DE EXECUÇÃO

10.1. A Contratada deverá apresentar ao Contratante, no prazo máximo de 15 (quinze) dias úteis, contados da data de assinatura do contrato, comprovante de prestação de garantia prévia correspondente ao percentual de 5% (cinco por cento) do valor global do contrato, podendo optar por uma das seguintes modalidades:

a) Caução em dinheiro;
b) Seguro garantia;
c) Fiança bancária.

10.1.1. Caso não haja, no prazo acima, possibilidade da apresentação da comprovação exigida no subitem 10.1, a Licitante deverá apresentar protocolo de solicitação.

10.1.2. No caso de a Contratada optar pelo seguro-garantia, poderá decidir-se por uma das seguintes alternativas:

a) Apresentar seguro-garantia para os riscos elencados no subitem 10.1.3, correspondente a 5% (cinco por cento) do valor global atualizado do contrato, na modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviço" com cláusula específica indicando a cobertura adicional de obrigações previdenciárias e/ou trabalhistas não honradas pela Contratada; ou
b) Apresentar seguro-garantia, modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviços" para cobertura constante nas alíneas "a" a "c" do subitem 10.1.3, complementada com a garantia adicional da modalidade "Seguro-Garantia de Ações Trabalhistas e Previdenciárias" para a alínea "d" do subitem 10.1.3, correspondente a 2% (dois por cento) e 3% (três por cento), respectivamente, do valor global atualizado do contrato.

10.1.3. A garantia, em qualquer das modalidades escolhidas, visa assegurar o pagamento de:

a) Eventual prejuízo decorrente do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações assumidas;
b) Eventuais prejuízos causados ao SESI – CN, ou terceiros, decorrentes de culpa ou dolo durante a execução do contrato;
c) Eventuais multas aplicadas pelo SESI-CN à Contratada; e
d) Obrigações e encargos trabalhistas, fiscais ou previdenciários de qualquer natureza, não honradas pela Contratada.

10.2. No caso de escolha da modalidade seguro-garantia, em seus termos deverá constar, expressamente, as previsões contidas nas alíneas "a" a "d" do subitem 10.1.3.

10.3. O descumprimento do prazo estabelecido no subitem 10.1 acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 10% (dez por cento).

10.4. O atraso superior a 15 (quinze) dias no cumprimento do estabelecido no subitem 10.1 poderá ensejar a rescisão do contrato por inadimplemento, sujeitando-se a Contratada às sanções estabelecidas no Regulamento de Licitações e Contratos do SESI.

10.5. A garantia emitida deverá conter, expressamente, declaração de que o responsável pela garantia possui plena ciência dos termos e condições deste instrumento convocatório.

10.6. A garantia será considerada extinta:

a) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do SESI-CN de que a Contratada cumpriu todas as cláusulas do contrato;
b) Ao final da vigência do Contrato.

10.7. A garantia deixará de ser executada nas seguintes hipóteses:

a) Caso fortuito ou força maior;
b) Alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;
c) Descumprimento das obrigações, pela Contratada, em decorrência de atos ou fatos praticados pelo SESI – CN;
d) Atos ilícitos dolosos praticados por colaboradores do SESI – CN.

10.8. Caberá ao SESI – CN apurar as isenções de responsabilidade previstas no subitem 10.7.

10.9. Não serão aceitas garantias que não as previstas neste instrumento convocatório.

10.10. Havendo a utilização da garantia para pagamento de multa que tenha sido aplicada à Contratada, esta deverá proceder à respectiva reposição no prazo de 05 (cinco) dias úteis contados da data em que for notificada da imposição da sanção.

10.11. A garantia será extinta com a emissão da DECLARAÇÃO de que a Contratada executou integralmente o objeto contratado, servindo para fins de autorização e levantamento da caução em dinheiro e extinção da garantia.

10.12. A DECLARAÇÃO de que trata o subitem anterior será emitida após o decurso do prazo de 120 (cento e vinte) dias da emissão do Termo de Encerramento de Contrato–TEC, desde que comprovado o pagamento de todas as verbas trabalhistas e previdenciárias decorrentes da contratação.

10.13. A licitante vencedora manterá a garantia de execução do contrato durante todo o prazo contratual, prorrogando-a, complementando-a ou substituindo-a, sempre com antecedência de 30 (trinta) dias à sua expiração.

10.14. A garantia deverá ser ajustada sempre que ocorrer o reajuste de preços ou eventuais diminuições de seu valor pela utilização nos casos previstos neste contrato.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa, o licitante/adjudicatário que:

11.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

11.1.2. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

11.1.3. apresentar documentação falsa;

11.1.4. fraudar na execução do contrato;

11.1.5. deixar de entregar os documentos exigidos no certame;

11.1.6. ensejar o retardamento da execução do objeto;

11.1.7. não mantiver a proposta;

11.1.8. cometer fraude fiscal;

11.1.9. comportar-se de modo inidôneo

11.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

11.3. A Contratada que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

11.3.1. Advertência por escrito.

11.3.2. Será aplicada multa pelo descumprimento dos prazos relacionados aos NÍVEIS DE ACORDO DE SERVIÇO do Termo de Referência, causado pela CONTRATADA. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

11.3.2.1. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

11.3.2.1.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,1% (um décimo por cento) ao dia do valor total do respectivo Contrato;

11.3.2.1.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea anterior será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total do respectivo Pedido de Compras / Contrato.

11.3.3. Será aplicada multa pelo atraso, causado pela CONTRATADA, no fornecimento das informações sobre os canais de atendimento. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

11.3.3.1. O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

11.3.3.1.1. Para atrasos de até 10 (dez) dias corridos, multa de 0,05% (cinco centésimos por cento) ao dia do valor total do respectivo Pedido de Compras / Contrato;

11.3.3.1.2. Para atrasos superiores a 10 (dez) dias corridos, a multa descrita na alínea anterior será substituída por multa de 0,1% (um décimo por cento) ao dia, até o limite máximo de 2% (dois por cento) do valor total do respectivo Contrato.

11.3.4. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 0,1% (um décimo por cento) à hora, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela CONTRATADA, no cumprimento dos prazos para solução das ocorrências, causado pela CONTRATADA, para cada chamado registrado pela CONTRATANTE. O descumprimento de mais de um prazo para um mesmo chamado implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

11.3.5. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia, até o limite máximo de 20% (vinte por cento), pelo atraso, causado pela CONTRATADA, no fornecimento da solução definitiva para as ocorrências de software. O descumprimento do prazo de cada chamado registrado pela CONTRATANTE implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

11.3.6. Será aplicada multa, calculada com base no valor do contrato em garantia do cumprimento das obrigações contratuais, de até 5% (cinco por cento), pelo atraso, causado pela CONTRATADA, no fornecimento de qualquer um dos relatórios solicitados, do Termo de Referência.

11.3.7. Será aplicada multa de 0,25% (vinte e cinco centésimos por cento) à 10% (dez por cento) do valor total do respectivo Pedido de Compras / Contrato pelo inadimplemento contratual relacionado às situações não previstas nos subitens anteriores.

11.3.8. As multas constantes nesse item poderão ser aplicadas cumulativamente conforme o caso e são meramente moratórias, não isentando a CONTRATADA o ressarcimento por perdas e danos pelos prejuízos a que der causa.

11.3.9. Caso o valor total pago mensalmente pela CONTRATANTE para manutenção dos equipamentos seja insuficiente para o débito das multas devidas pela CONTRATADA no referido mês, o valor devido deverá ser descontado integralmente do valor caucionado em garantia do cumprimento das obrigações contratuais.

11.3.10. Ao término dos prazos previstos, contados a partir da emissão da Ordem de Serviço, poderá ser aplicada multa moratória de 0,50% (cinquenta centésimos por cento), em cima do valor de cada item avaliado, por dia de atraso.

11.3.11. Rescisão unilateral do contrato no caso de reincidência.

11.3.12. Pela rescisão do contrato por iniciativa da CONTRATADA, sem justa causa, responderá esta por perdas e danos que a rescisão ocasionar ao SESI/CN.

11.3.13. Suspensão temporária do direito de participar em licitações e impedimento de contratar com o SESI/CN, por prazo não superior a 2 (dois) anos.

11.4. As multas serão descontadas dos pagamentos a que a CONTRATADA fizer jus, ou recolhidas diretamente à Tesouraria do SESI/CN, no prazo de 15 (quinze) dias, contados a partir da data de sua comunicação, ou, ainda, quando for o caso, cobradas judicialmente.

11.5. Para a aplicação das penalidades aqui previstas, a CONTRATADA será notificada para apresentação de defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir da notificação.

11.6. As penalidades previstas neste contrato são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis, tantas vezes quantas forem as irregularidades constatadas.

11.7. A CONTRATADA deverá comunicar ao SESI/CN, por escrito e justificadamente, as ocorrências de caso fortuito ou de força maior impeditivas do cumprimento do objeto contratado, no prazo máximo improrrogável de 2 (dois) dias úteis, contados da data da ocorrência, sob pena de não poder alegá-los posteriormente.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO CONTRATUAL

12.1. Pelo descumprimento de quaisquer de suas cláusulas e condições, poderá o SESI/CN rescindir o presente contrato, independentemente de prévia interpelação judicial, respondendo a CONTRATADA pelos prejuízos ocasionados, ressalvadas as hipóteses de caso fortuito ou força maior, desde que devidamente comprovados.

12.2. O SESI/CN, a seu livre critério e quando bem lhe convier, poderá dar por findo o presente contrato independentemente de justo motivo, e sem que lhe caiba qualquer sanção, desde que o faça mediante comunicação prévia e por escrito, à CONTRATADA, de 120 (cento e vinte) dias.

12.3. Rescindido o presente contrato por culpa da CONTRATADA, o SESI/CN entregará o objeto deste instrumento a quem julgar conveniente, sem qualquer consulta ou interferência da CONTRATADA, que responderá na forma legal e contratual pela infração ou execução inadequada que tenha dado causa à rescisão.

12.4. Fica, ainda, estabelecido que o SESI/CN poderá considerar igualmente rescindido o contrato independentemente de qualquer aviso extrajudicial ou interpelação judicial, nos seguintes casos:

12.4.1. Transferência do contrato, por meio de cessão, transferência ou subcontratação, no todo ou em parte, a terceiros, sem a prévia e expressa autorização do SESI/CN;

12.4.2. Caução ou utilização do contrato, para qualquer operação financeira, sem a prévia e expressa autorização do SESI/CN.

12.5. Pelo atraso injustificado ou paralisação no fornecimento dos serviços, sem a devida justificativa e a prévia comunicação à CONTRATANTE.

12.6. Pelo atraso superior a 60 (sessenta) dias dos pagamentos devidos pela CONTRATANTE, decorrentes de fornecimento já recebido e aceito, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao SESI, o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

12.7. Pela não liberação, por parte da CONTRATANTE, de área ou local para instalação de equipamentos e para execução dos serviços objeto deste Contrato.

CLÁUSULA DÉCIMA TERCEIRA – DO ACORDO DE NÍVEIS DE SERVIÇO (ANS)

13.1. Os Acordos de Níveis de Serviço (ANS) são aqueles previstos no Termo de Referência, anexo do Edital.

CLÁUSULA DÉCIMA QUARTA - DA NOVAÇÃO

14.1. A omissão ou tolerância do SESI/CN, em exigir o estrito cumprimento dos termos e condições deste Contrato, não constituirá novação ou renúncia, nem afetará os seus direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA DÉCIMA QUINTA - DA CONFIDENCIALIDADE

15.1. A CONTRATADA se obriga a guardar sigilo dos dados e informações aos quais venha a ter acesso em razão deste CONTRATO obrigando-se ainda a não permitir que nenhum de seus empregados ou terceiros sob a sua responsabilidade façam uso destas informações para fins diversos do objeto contratual.

15.2. Fica desde já acordado que os termos e condições deste CONTRATO, bem como quaisquer operações, métodos, procedimentos, dados, informações, sistemas, softwares, documentos, metodologias, inovações, especificações técnicas e comerciais, materiais, dispositivos, inovações, marcas, criações, especificações, de caráter técnico ou comercial, que venham a ter acesso ou conhecimento, em razão deste ajuste, são estritamente confidenciais, e não serão publicados ou divulgados, sob qualquer forma, a terceiros.

15.3. A obrigação quanto à confidencialidade permanecerá em vigor por tempo indeterminado, até que o CONTRATANTE, expressamente e por escrito, resolva por sua extinção.

15.4. A CONTRATADA se compromete a preservar o caráter sigiloso de toda e qualquer informação considerada confidencial por si, seus empregados, administradores, prepostos, representantes de qualquer natureza, contratados e subcontratados.

CLÁUSULA DÉCIMA SEXTA – DOS PODERES

16.1. As partes contratantes declaram, sob as penas da lei, que os signatários do presente instrumento são seus procuradores/representantes legais, devidamente constituídos na forma dos respectivos instrumentos constitutivos, contratos/estatutos sociais, com poderes para assumirem as obrigações ora contratadas, devendo, as partes, apresentarem cópias destes instrumentos e do Cadastro Nacional de Pessoa Jurídica – CNPJ.

CLÁUSULA DÉCIMA SÉTIMA – DO FORO

17.1. As partes elegem o Foro da Circunscrição Judiciária de Brasília/DF, com renúncia a qualquer outro, por mais privilegiado que seja, para dirimir as questões que, porventura, surgirem na execução do presente contrato. E assim, por estarem justos e acertados, assinam as partes o presente instrumento, em 2 (duas) vias de igual teor e forma, para um só efeito, sem rasuras ou emendas, na presença das testemunhas abaixo nomeadas, para que produza seus efeitos jurídicos.

Brasília, XXX de XXX de 2021.

Pelo SESI - CONSELHO NACIONAL _____ **PEDRO ANTÔNIO FIORAVANTE SILVESTRE NETO** **Superintendente Executivo**	**Pela CONTRATADA** _____ **XXXXXXX**
Testemunhas **Nome:** **CPF:**	 **Nome:** **CPF:**