EDITAL DE PREGÃO ELETRÔNICO
PREÂMBULO

CÓDIGO DO ÓRGÃO	**XXXXXXXX**
OBJETO	Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital
MODALIDADE DE LICITAÇÃO:	PREGÃO ELETRÔNICO Nº 046/CPB/2024
PROCESSO ADMINISTRATIVO Nº:	0696/2024
AMBIENTE ELETRÔNICO	www.licitacoes-e.com.br
RETIRADA DO EDITAL	Presencial e/ou por meio de baixa de arquivos digitais pelos endereços eletrônicos: www.licitacoes-e.com.br e www.cpb.org.br
TELEFONE DE CONTATO	(11) 4710 – 4129
INÍCIO DO PRAZO DE ENVIO DE PROPOSTAS ELETRÔNICAS	24 de julho de 2024.
ABERTURA DA SESSÃO PÚBLICA DE PROCESSAMENTO DO CERTAME	07 de agosto de 2024, às 10h30.

O **COMITÊ PARALÍMPICO BRASILEIRO** torna público, para conhecimento de quantos possam se interessar, em acordo com as disposições contidas neste termo de convocação, no Regulamento de Aquisições e Contratos/RAC, aprovada pela Resolução CPB nº 01 de 03 de abril de 2023, subsidiariamente pela Lei 14.133/2021, INSTRUÇÃO NORMATIVA SEGES/ME Nº 73/22 e da Lei Complementar nº 123/2006 e suas atualizações, fará realizar licitação na modalidade **PREGÃO**, a ser realizada por intermédio do sistema eletrônico de contratações denominado **"LICITAÇÕES-E"**, com utilização de recursos de tecnologia da informação, denominada **PREGÃO ELETRÔNICO**, do tipo **MENOR VALOR TOTAL**, a ser processada pela Comissão Permanente de Licitação deste Comitê, em conformidade com as disposições deste edital e respectivos anexos.

As propostas deverão obedecer às especificações deste instrumento convocatório e seus anexos e serão encaminhadas por meio eletrônico, após o registro dos interessados em participar do certame e o credenciamento de seus representantes, no LICITAÇÕES-E, do Portal do Banco do Brasil.

A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico www.licitacoes-e.com.br , no dia e hora mencionados no preâmbulo deste Edital e será conduzido pelo pregoeiro com o auxílio da equipe de apoio, designados na portaria CPB nº 035 de 08 de maio de 2024 e indicados no sistema pela autoridade competente.

1. DO OBJETO

1.1 A presente licitação tem por objeto a **Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital**, em conformidade com as especificações técnicas constantes do Termo de Referência que integra o presente Edital de Licitação **Pregão Eletrônico nº 046/CPB/2024**, como Anexo I.

2. DA PARTICIPAÇÃO

2.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema **LICITAÇÕES-E**, em atividade econômica compatível com o seu objeto, sejam detentores de senha para participar de procedimentos eletrônicos, na forma estabelecida no regulamento que disciplina a inscrição no referido Cadastro;

2.2. Será concedido tratamento diferenciado para as microempresas que se enquadram na condição de empresas de pequeno porte e microempreendedores individuais, nos termos da Lei Complementar nº 123/06;

2.3. A licitante responde integralmente por todos os atos praticados na sessão pública do pregão eletrônico, por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante;

2.4. Cada representante credenciado poderá representar apenas uma licitante, em cada pregão eletrônico;

2.5. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

2.6. Não será admitida a participação, neste certame licitatório, dos interessados:

2.6.1. Que se encontre impossibilitada de participar da licitação e de celebrar contratos administrativos, na forma da legislação vigente, em decorrência de sanção que lhe foi imposta;

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

2.6.3. Que se enquadrem nas vedações previstas no artigo 14 da Lei n° 14.133, de 2021;

2.6.4. Que estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

2.6.4.1. Caso a empresa esteja em processo de recuperação judicial, deverá ser apresentada a certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório nos termos da Lei Federal nº 14.133/2021;

2.6.5. Que mantenham vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do CPB ou com agente que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.7. Tenham sido proibidos pelo Plenário do CADE de participar de licitações promovidas pela Administração Pública federal, estadual, municipal, direta e indireta, em virtude de prática de infração à ordem econômica, nos termos do artigo 38, inciso II, da Lei Federal n° 12.529/2011;

2.6.8. Dirigentes, bolsistas ou empregados da entidade;

2.6.9. Fornecedores que tenham perdido ou estejam suspensos no direito de contratar com o CPB;

2.6.10. Que estejam com o direito de licitar e contratar temporariamente suspenso, ou que estejam impedidas de licitar e contratar com a Administração Pública Federal ou com o CPB;

2.6.11. Que estejam reunidas em consórcio ou sejam controladoras, coligadas ou subsidiárias entre si;

2.6.12. Que possuam sócios ou funcionários com vínculo empregatício com o Comitê Paralímpico Brasileiro ou com as Entidades de Administração do Desporto;

2.6.13. Outros casos identificados, inclusive no decorrer do certame, mediante justificativa da Comissão de Aquisição ou do Pregoeiro.

3. DO CREDENCIAMENTO NO SISTEMA E DAS PROPOSTAS ELETRÔNICAS

3.1. DO CREDENCIAMENTO NO SISTEMA

3.1.1. Para acesso ao Sistema eletrônico, os interessados em participar do Pregão deverão fazer o seu pré-cadastramento junto ao Banco do Brasil, devendo se dirigir a uma agência do Banco do Brasil - provedor do Sistema Eletrônico de Compras "Licitações-E" - e preencher os formulários próprios.

3.1.2. Os licitantes interessados deverão credenciar representantes, mediante a apresentação de procuração por instrumento público ou particular, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no "licitações-e".

3.1.3. Em sendo sócio, proprietário, dirigente (ou assemelhado) da empresa proponente, deverá apresentar cópia do respectivo Estatuto ou Contrato Social, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura.

3.1.4. A chave de identificação e a senha poderão ser utilizadas em qualquer Pregão Eletrônico dentro do Portal "**LICITAÇÕES-E**", salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco.

3.1.5. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao COMITÊ PARALÍMPICO BRASILEIRO (CPB) a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.1.6. É vedado o credenciamento de um mesmo representante para duas ou mais empresas.

3.1.7. O credenciamento da empresa e de seu representante legal junto ao Sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica e habilitatória para realização das transações inerentes ao Pregão Eletrônico.

3.2. **DAS PROPOSTAS ELETRÔNICAS**

3.2.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico os documentos de habilitação exigidos no edital e proposta com a descrição do objeto ofertado, quando solicitado pelo Pregoeiro.

3.2.2. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

3.2.3. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, conforme legislação.

3.2.4. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

3.2.4.1. Valor **UNITÁRIO** E **TOTAL DO LOTE**;

3.2.4.2. Descrição detalhada do objeto, conforme requer este Edital e o Termo de Referência;

3.2.5. As propostas devem ser elaboradas por preço único, conforme solicitado na proposta, incluindo todo material necessário, como também toda mão de obra necessária para execução do serviço, seguindo as especificações técnicas contidas no Termo de Referência (anexo I deste Edital).

3.2.6. Como condição para participação no Pregão, o licitante deverá declarar em campo próprio do sistema eletrônico, relativo às seguintes declarações:

3.2.6.1. 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 47.

3.2.6.2. A falta da declaração apenas produzirá o efeito de o licitante não ter direito ao tratamento diferenciado previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa e empresa de pequeno porte;

3.2.6.3. Que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

3.2.6.4. Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores.

3.2.6.5. A falsidade das declarações prestadas, objetivando os benefícios da Lei Complementar nº 123/06, poderá caracterizar o crime de que trata o artigo 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das sanções previstas na legislação pertinente e, neste edital, e mediante o devido processo legal, e implicará, também, a inabilitação do licitante, se o fato vier a ser constatado durante o trâmite da licitação.

3.2.7. O licitante deverá informar no campo "Informações Adicionais" do Formulário Eletrônico da Proposta (tal formulário é disponibilizado para os fornecedores quando efetuam o "acesso identificado" no site www.licitacoes-e.com.br), que atende plenamente as especificações dos serviços, de acordo com o Edital. A falta dessa informação não acarretará a desclassificação do licitante, visto que a inserção de proposta no Sistema Eletrônico do Banco do Brasil, indica que o licitante está ciente destas condições, não podendo alegar desconhecimento das informações contidas no Edital e de seus deveres, em nenhuma hipótese.

3.2.7.1. É VEDADA A INCLUSÃO DE QUALQUER IDENTIFICAÇÃO DO LICITANTE NA PROPOSTA EVENTUALMENTE ANEXADA AO SISTEMA 'licitacoes-e'. Caso o Pregoeiro verifique alguma identificação, tanto nas 'informações adicionais' quanto na eventual proposta anexada, o licitante será DESCLASSIFICADO.

3.2.8. Todas as especificações do objeto contidas na proposta vinculam a licitante contratada.

3.2.9. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

3.2.10. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, caso o previsto não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados no artigo 107 da Lei n° 14.133, de 2021.

3.2.11. Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da contratante, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário.

3.2.12. Em se tratando de Microempreendedor Individual – MEI, o licitante deverá incluir, no campo das condições da proposta do sistema eletrônico, o valor correspondente à contribuição prevista no art. 18-B da Lei Complementar n. 123, de 2006.

3.2.13. O prazo de validade da proposta não será inferior a 180 (cento e oitenta) dias, a contar da data de sua apresentação.

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

3.2.15. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de classificação e fase de lances.

4. DA HABILITAÇÃO

4.1. O julgamento da habilitação se processará mediante a análise dos documentos a seguir relacionados, os quais dizem respeito a:

4.1.1. HABILITAÇÃO JURÍDICA

a) Registro empresarial na Junta Comercial, no caso de empresário individual e Sociedade Limitada Unipessoal – SLU", conforme a Lei n. 13.874/19 e a Lei n. 14.195/2021;

b) Ato constitutivo, estatuto ou contrato social atualizado e registrado na Junta Comercial, em se tratando de sociedade empresária;

c) Documentos de eleição ou designação dos atuais administradores tratando-se de sociedades empresárias;

d) Ato constitutivo atualizado e registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

e) Decreto de autorização em se tratando de sociedade empresária estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

4.1.2. REGULARIDADE FISCAL E TRABALHISTA

a) Prova de inscrição no Cadastro de Contribuintes Estadual e Municipal, relativo à sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual, ou prova de sua isenção, se for o caso;

b) Prova de regularidade para com as Fazendas Federal, Estadual e Municipal, como segue:

b.1) Certidão negativa, ou positiva com efeitos de negativa, de débitos relativos a Créditos Tributários Federais e dívida ativa da União;

b.2) Certidão de regularidade de débitos tributários com a Fazenda Estadual da sede da licitante;

b.2.1) No caso de a licitante ter domicílio ou sede no Estado de São Paulo, a prova de regularidade para com a Fazenda Estadual se dará através da certidão negativa de débitos tributários da Dívida Ativa do Estado de São Paulo, expedida pela Procuradoria Geral do Estado, conforme Portaria CAT 20/98.

b.3) Certidão de regularidade de débitos tributários com a Fazenda Municipal da sede da licitante;

b.3.1) No caso de a licitante ter domicílio ou sede no Município de São Paulo, a prova de regularidade para com a Fazenda Municipal se dará através de Certidão Conjunta de Débitos de Tributos Mobiliários.

b.3.2) Caso a licitante não esteja cadastrada como contribuinte no Município de São Paulo, deverá apresentar declaração firmada pelo seu representante legal/procurador, sob as penas da lei, do não cadastramento e de que nada deve à Fazenda do Município de execução dos serviços, sem prejuízo da apresentação da certidão referente a sua sede ou domicílio, de acordo com o modelo constante do Anexo III deste Edital.

c) Certificado de Regularidade de Situação para com o Fundo de Garantia de Tempo de Serviço (CRF – FGTS);

d) Certidão negativa, ou positiva com efeitos de negativa, de débitos trabalhistas (CNDT);

e) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ do Ministério da Fazenda, devidamente ativo.

4.1.2.1. Se a licitante for a matriz, todos os documentos deverão estar em nome da matriz;

4.1.2.2. Se a licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles que pela própria natureza, forem comprovadamente emitidos apenas em nome da matriz.

4.1.3. **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

4.1.3.1 Certidão negativa de falência, recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica ou do domicílio do empresário individual;

4.1.3.2 Caso o licitante esteja em recuperação judicial ou extrajudicial, deverá ser comprovado o acolhimento do plano de recuperação judicial ou a homologação do plano de recuperação extrajudicial, conforme o caso.

4.1.3.3 Se a licitante for sociedade não empresária, a certidão mencionada na alínea "a" deverá ser substituída por certidão negativa de ações de insolvência civil.

4.1.4. **DECLARAÇÕES E OUTRAS COMPROVAÇÕES**

4.1.4.1. Declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **Anexo IV** atestando que para fins do disposto no inciso IV do art. 63 da Lei Federal n.º 14.133/2021, cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

4.1.4.2. Declaração subscrita por representante legal da licitante, em conformidade com os modelos constantes do **Anexo V**, afirmando que sua proposta foi elaborada de maneira independente e que conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira e ao CPB, em atendimento à Lei Federal nº 12.846/ 2013 – Lei Anticorrupção.

4.1.4.3. Ficha de Cadastro de Fornecedor, conforme **Anexo VI**.

4.1.5. Questionário de Due Diligence, conforme anexo VII, a avaliação do Questionário será realizada pelo Departamento de Compliance do CPB, que emitirá uma recomendação sobre contratar com o terceiro ou não, que, em caso negativo, será submetida à Diretoria Executiva do CPB. A Diretoria Executiva do CPB poderá vetar a contratação com base na avaliação do Questionário de Due Diligence, o que importará na inabilitação da licitante, sendo oportunizado o contraditório e ampla defesa no momento destinado ao recurso no procedimento de licitação.

4.1.6. **DA QUALIFICAÇÃO TÉCNICA**

4.1.6.1 Atestado(s) /certidão(ões), em nome da licitante, fornecido (s) por pessoa jurídica de direito público ou privado, que comprove(m) fornecimento de 50% (cinquenta por cento) do objeto desta licitação: Prestação de serviços em fornecimento de firewall e antivírus com características similares ao solicitado neste Termo de Referência, ou seja, que tenham características de atendimento para grandes empresas.

4.1.6.2 O(s) atestado(s) ou certidão(ões) deverá(ão) ser assinado (s) por autoridade ou representante de quem o (s) expediu, com a devida identificação.

4.1.6.3 Para fins de comprovação de qualificação técnica, será considerada a somatória dos atestados, podendo ser apresentados documentos diversos que relatem o fornecimento do objeto licitatório.

5. DA SESSÃO PÚBLICA E DO JULGAMENTO

5.1. O Pregoeiro, a seu critério, poderá diligenciar para esclarecer dúvidas ou obter a confirmação do teor das declarações e comprovações elencadas no item IV deste Edital, aplicando-se, em caso de falsidade, as sanções penais e administrativas pertinentes, garantidos os direitos ao contraditório e a ampla defesa.

5.2. Na hipótese de convocação das licitantes classificadas remanescentes, deverão ser retomados os procedimentos cabíveis, em sessão pública, procedendo-se conforme especificações deste edital.

5.3. Abertura das propostas: No dia e horário previstos neste edital, o Pregoeiro designado para condução do certame dará início à sessão pública do pregão eletrônico, passando a avaliar a aceitabilidade das propostas.

5.3.1. **Análise:** A análise das propostas pelo Pregoeiro visará ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente.

5.3.2. Serão desclassificadas as propostas:

a) Que contiverem vícios insanáveis;

b) Não obedecerem às especificações técnicas pormenorizadas no edital;

c) Apresentarem preços inexequíveis ou permanecerem acima do orçamento estimado para a contratação;

d) Não tiverem sua exequibilidade demonstrada, quando exigido pelo CPB;

e) Apresentarem desconformidade com quaisquer outras exigências do edital, desde que insanável.

5.3.3. A desclassificação se dará por decisão motivada do Pregoeiro, observado o disposto no artigo 59, §2º, da Lei Federal nº 14.133/2021.

5.3.4. O eventual desempate de propostas do mesmo valor será promovido pelo sistema, com observância dos critérios legais estabelecidos para tanto.

5.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.5. Após a fase de "Classificação das Propostas", o Pregoeiro dará sequência ao processo de Pregão, passando para a fase da "Sessão Pública" (LANCES), da qual só poderão participar os licitantes que tiveram suas propostas classificadas.

5.6. Na etapa competitiva, que será aberta com o menor preço ofertado na fase de inserção de propostas, os representantes dos licitantes deverão estar conectados ao Sistema para participar da sessão de lances. A cada lance ofertado o licitante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

5.6.1. O Sistema eletrônico aceita e registra lances cujos valores forem inferiores ao último lance do próprio licitante ou de seus concorrentes.

5.6.2. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

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

5.6.4. A Licitante somente poderá oferecer lance inferior ou percentual de desconto maior ao último por ela ofertado e registrado pelo sistema, observado o intervalo mínimo de:

LOTE ÚNICO: R$ 9.000,00 (nove mil reais).

5.6.5. O encerramento da etapa normal de lances será decidido pelo Pregoeiro, que informará, sobre o início do modo randômico.

5.6.5.1. Decorrido o prazo fixado pelo Pregoeiro, o Sistema eletrônico encaminhará aviso de encerramento do modo normal da disputa, após o que transcorrerá período randômico (aleatório), que pode variar de 1 segundo a 30 (trinta) minutos, aleatoriamente

determinado pelo Sistema, findo o qual será automaticamente encerrada a fase de disputa de lances.

5.6.5.2. O tempo randômico é gerado pelo Sistema, não sendo possível ao Pregoeiro, ou a qualquer outra pessoa, sua administração.

5.6.6. Se algum licitante fizer um lance que esteja em desacordo com a licitação (preços e diferenças inexequíveis ou excessivas) poderá tê-lo cancelado pelo Pregoeiro através do Sistema. Na tela será emitido um aviso e na sequência o Pregoeiro justificará o motivo da exclusão através de mensagem aos licitantes.

5.6.7. O Sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo Pregoeiro acerca da aceitação do lance de menor valor.

5.6.8. No caso de não haver lances na "Sessão Pública", serão considerados os valores obtidos na etapa de "Abertura das Propostas".

5.6.9. Ao final da sessão pública (LANCES), o sistema informará a proposta de menor preço e seu autor, bem como a nova ordem classificatória. O Pregoeiro convocará o licitante vencedor para apresentar documentos e proposta atualizada.

5.7. **Empate ficto**: 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.

5.7.1. 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.

5.7.2. A mais bem 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 05 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.7.3. Caso a microempresa e empresa de pequeno porte melhor classificada 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.

5.7.4. 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.

5.7.5. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei n° 14.133, de 2021.

5.7.6. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

5.7.7. Independente da condição especial de Microempresa ou Empresa de Pequeno Porte, a empresa melhor classificada deverá atender, na íntegra, a exigência dos itens deste Edital.

5.7.8. Havendo alguma restrição na comprovação da regularidade fiscal das empresas enquadradas como ME ou EPP, será assegurado o prazo de 05 (cinco) dias úteis, após a declaração do vencedor, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, podendo ser prorrogado por mais 05 (cinco) dias úteis, a critério do Pregoeiro.

5.7.8.1. A não-regularização da documentação, nos termos do item anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital.

5.7.8.2. Não se concretizando a contratação da microempresa ou empresa de pequeno porte, a autoridade competente decidirá motivadamente pela revogação ou pelo prosseguimento da licitação.

5.7.8.3. Na hipótese de microempresa ou empresa de pequeno porte ter se sagrado vencedora da licitação, com o benefício do empate ficto previsto no § 2º do artigo 44 da Lei Complementar nº 123/06, poderão ser convocadas as remanescentes que porventura se enquadrem na situação do empate ficto, na ordem classificatória, para o exercício do mesmo direito, desconsiderado o preço ofertado no primeiro empate, garantidos os mesmos prazos inicialmente concedidos. Não havendo o exercício do benefício do desempate por microempresa ou empresa de pequeno porte ou sua efetiva contratação, o objeto licitado poderá ser adjudicado em favor da proposta originalmente vencedora do certame, nos termos do disposto no § 1º do artigo 45 da Lei complementar nº 123/06.

5.7.8.4. No caso de microempresa ou empresa de pequeno porte ter se sagrado vencedora da licitação por ter sido desde logo a mais bem

classificada, poderão ser convocadas os licitantes remanescentes, na ordem classificatória, para o prosseguimento do certame ou da contratação, conforme o caso, sem a aplicação do benefício do empate ficto. O Pregoeiro examinará as ofertas subsequentes até a apuração de uma que atenda ao Edital, podendo, inclusive, negociar diretamente com o proponente para que seja obtido preço melhor.

5.7.8.5. Aplica-se o disposto também às hipóteses de inabilitação de microempresa e empresa de pequeno porte mais bem classificada.

5.8. Encerrada a etapa de disputa de lances o Pregoeiro solicitará os documentos de habilitação conforme disposto no Edital e seus anexos, devendo o licitante melhor classificado enviar os documentos de habilitação no prazo de 1h (uma hora), sob pena de inabilitação.

5.8.1. Em casos específicos, ou que o sistema eletrônico venha a apresentar algum tipo de oscilação/quedas ou qualquer outro problema, o pregoeiro poderá permitir que envio dos documentos de habilitação e os demais anexos, sejam enviados para o e-mail pregao@cpb.org.br.

5.8.2. Os documentos recebidos por e-mail serão disponibilizados no endereço https://cpb.org.br/licitacoes/ ainda no curso da sessão pública para acesso de todos os participantes.

5.8.3. Os documentos necessários à habilitação deverão, sob responsabilidade pessoal do licitante ou seu representante, ser apresentados via sistema eletrônico, desde que contenham assinatura digital de seus representantes, dispensando-se o envio físico dos originais ou cópias autenticadas.

5.8.3.1. Em caso de dúvida quanto à autenticidade do documento, o pregoeiro abrirá prazo de dois dias úteis para apresentação do documento original.

5.8.4. O Pregoeiro poderá solicitar no chat de mensagens aberto no Sistema, desde o encerramento da disputa até a efetiva homologação do processo licitatório, a documentação das demais licitantes classificadas, obedecendo a ordem de classificação, para garantir a execução do objeto dentro das exigências do Edital. As empresas convocadas que não apresentarem a documentação estarão sujeitas às penalidades previstas neste Edital, ficando de inteira responsabilidade dos licitantes o acompanhamento das mensagens e dos resultados naquele Sistema até a homologação do certame.

5.8.5. Será desclassificada a proposta ou o lance vencedor com valor superior ao preço máximo fixado ou que apresentar preço manifestamente inexequível.

5.8.5.1. Considera-se inexequível a proposta que apresente preço global ou unitário simbólico irrisório ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

5.8.6. Se a proposta ou o lance de menor valor não for aceitável, ou se o licitante desatender às exigências habilitatórias, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua compatibilidade e a habilitação do licitante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda o Edital. Também nessa etapa o Pregoeiro poderá negociar com o licitante para que seja obtido preço melhor.

5.8.7. O Pregoeiro poderá a qualquer momento solicitar às licitantes os esclarecimentos que julgar necessários.

5.8.8. A critério do Pregoeiro, a sessão pública poderá ser suspensa por até 02 (dois) dias úteis para a apresentação da planilha de proposta em conformidade com o modelo do Anexo II.

5.8.9. Constatando o atendimento das exigências fixadas neste Edital, o licitante será declarado VENCEDOR e, transcorridas as fases e os prazos legais, o objeto será adjudicado ao autor da proposta ou lance de menor preço.

5.9. O Pregoeiro convocará o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema estabelecendo no "chat" prazo razoável para tanto, que será de 01:00 (uma hora), sob pena de não aceitabilidade da proposta.

5.9.1. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

5.9.2. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por igual período, mediante solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

5.10. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

5.11. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade dela.

5.12. Nos itens não exclusivos a microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, seguindo-se a disciplina antes estabelecida, se for o caso.

6. DO RECURSO, DA ADJUDICAÇÃO, DA HOMOLOGAÇÃO E CONVOCAÇÃO PARA ASSINATURA DO CONTRATO.

6.1. Divulgado o vencedor ou, se for o caso, saneada a irregularidade fiscal o Pregoeiro informará às licitantes, por meio de mensagem lançada no sistema, que poderão interpor recurso, imediata e motivadamente, por meio eletrônico, utilizando para tanto, exclusivamente, campo próprio disponibilizado no sistema, em até 20 (vinte) minutos após a decisão de habilitação (definida no sistema licitacoes-e como "Declarada Vencedora"), manifestando obrigatoriamente sua intenção de recurso, sob pena de preclusão (conforme art. 165, §1º, I, da Lei 14.133/21), com registro da síntese das suas razões, no campo apropriado do Sistema ("acolhimento de recurso"). O Pregoeiro fará análise da motivação da intenção de recurso, procedendo então sua aceitabilidade ou cancelamento.

6.1.1. Não serão conhecidos os recursos apresentados fora do prazo legal estabelecido em Edital e/ou subscritos por representante não habilitado legalmente ou não identificado no processo para responder pelo licitante.

6.1.2. Caso o recurso seja intempestivo ou não se comprove a representatividade legal do signatário, o CPB, de ofício, fará análise preliminar para verificar se há ilegalidade na decisão, e deixará de analisar o mérito, caso o conteúdo seja manifestamente protelatório.

6.2. Havendo manifestação indicando intenção em recorrer, na forma indicada no subitem 6.1, o Pregoeiro, por mensagem lançada no sistema, informará aos recorrentes que poderão apresentar as razões de recurso, no prazo de até 3 (três) dias úteis após o encerramento da sessão pública, e às demais licitantes que poderão apresentar contrarrazões, em igual prazo, os quais começarão a correr do término do prazo para apresentação das razões, sendo-lhes assegurada vistas dos autos, após o Pregoeiro declarar o vencedor", alterando o status do licitante arrematante para "Declarado Vencedor" no Sistema eletrônico www.licitacoes-e.com.br. A vista se dará no endereço da unidade promotora da licitação, ou seja, no Departamento de Aquisições e Contratos – DEAC do Comitê Paralímpico Brasileiro - CPB, localizado no Centro de

Treinamento Paraolímpico, sito a Rodovia dos Imigrantes, Km 11,5, CEP 04329-000, Vila Guarani, São Paulo, de 2ª a 6ª feira, das 09:00 às 12:00 e das 13:00 às 18:00.

6.2.1. As razões de recurso e as contrarrazões serão oferecidas exclusivamente por meio eletrônico, no sistema LICITAÇÕES-E, "Acolhimento de Recurso". Não será aceita manifestação fora do local determinado pelo sistema ("acolhimento de recurso"), ou seja, não será aceito por e-mail, telefone, pessoalmente ou via chat de mensagem.

6.2.2. O recurso terá efeito suspensivo e o seu acolhimento importará a invalidação dos atos insuscetíveis de aproveitamento.

6.2.3. A falta de interposição na forma prevista no subitem 6.1 importará a decadência do direito de recorrer e o pregoeiro adjudicará o objeto do certame ao vencedor, na própria sessão, propondo à autoridade competente a homologação do procedimento licitatório.

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

6.4. A adjudicação será feita pelo preço global, considerando a somatória e descrição dos valores unitários que o compõe, conforme detalhamento constante do Termo de Referência.

6.5. A(s) vencedora(s) do certame obrigam-se a apresentar, no prazo de até 02 (dois) dias úteis contado da data de adjudicação do objeto, os novos preços unitários com sua composição e o total para a contratação, conforme solicitação do pregoeiro, a partir do valor final obtido no certame.

6.5.1. Esses novos preços serão apresentados pela licitante vencedora, em nova planilha com assinatura e deverá ser encaminhada na forma eletrônica, aceita no edital ou diretamente no Departamento de Aquisições e Contratos – DEAC.

7. DA DESCONEXÃO COM O SISTEMA ELETRÔNICO

7.1. Ao licitante caberá acompanhar as operações no sistema eletrônico, durante a sessão pública, respondendo pelos ônus decorrentes de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

7.2. A desconexão do sistema eletrônico com qualquer licitante não prejudicará a conclusão e validação da sessão pública ou do certame.

8. DO PRAZO, DO LOCAL E DAS CONDIÇÕES DE EXECUÇÃO DO SERVIÇO

8.1. O objeto desta licitação deverá ser executado nos prazos, condições e locais indicados no Termo de Referência, que constitui Anexo I deste Edital, correndo por conta da contratada todas as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da prestação dos serviços.

8.2. O presente contrato vigorará por 12 (doze) meses, contados a partir da data de sua assinatura, podendo a contratação ser prorrogada, mediante a celebração de termo aditivo, limitado o somatório do tempo das prorrogações ao máximo de 120 (cento e vinte) meses, contados da data da celebração do contrato.

8.3. Após a execução dos serviços, deverá ser entregue a seguinte documentação pelo Contratado:

8.3.1. Via da Nota Fiscal com identificação do Número do Contrato;

8.3.1.1. Na hipótese de existir Nota de Retificação e/ou Nota Suplementar de Ordem de Início ou Termo de Contrato Assinado, as cópias(s) deverá(ão) acompanhar os demais documentos citados;
8.3.1.2. Fatura, quando couber;
8.3.1.3. Relatório descritivo dos serviços prestados;

9. DA EXECUÇÃO DOS SERVIÇOS

9.1. A efetivação da prestação dos serviços será aceita consoante ao disposto no art. 140 da Lei Federal nº 14.133/21.

9.2. Caso seja constatado irregularidades na execução dos serviços, não atendendo às especificações descritas na proposta, o Departamento solicitante deverá rejeitá-lo no todo ou em parte, determinando sua substituição/reparação ou apontando em relatório para que seja corrigido o vício constatado, mantido os valores inicialmente contratados, sem prejuízo das sanções previstas neste Edital e na legislação vigente.

9.2.1. O Departamento solicitante deverá prontamente informar o Departamento de Aquisição e Contratos quando constatada qualquer incompatibilidade na execução dos serviços prestados, com as características e danos registrados por meio de relatório circunstanciado.

9.3. O aceite definitivo ocorrerá mediante conferência e, posteriormente, caso a execução dos serviços esteja a contento, atesto da Nota Fiscal e encaminhará ao setor competente para realização do pagamento.

9.4. Havendo inexecução da prestação dos serviços o valor respectivo será descontado da importância devida à contratada, sem prejuízo da aplicação das sanções cabíveis.

9.5. Durante a vigência do contrato, é vedado ao contratado contratar cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, devendo essa proibição constar expressamente do edital de licitação.

9.6. Não será permitida a subcontratação total ou parcial do objeto do Contrato, salvo mediante prévia solicitação da CONTRATADA e sob autorização da CONTRATANTE.

10. DOS PAGAMENTOS

10.1. O prazo de pagamento será de até 30 (trinta) dias, a contar do atesto da nota fiscal pelo fiscal e/ou responsável do CPB, acompanhada obrigatoriamente dos documentos de: regularidade fiscal e trabalhista, conforme Regulamento de Aquisições e Contratos - CPB, devendo a retenção ser efetuada, conforme responsabilidade prevista na lei, na fonte dos tributos e contribuições determinadas pelos órgãos fiscais e fazendários em conformidade com a legislação vigente.

10.1.1. A discriminação do objeto, valor unitário e total, deverão ser reproduzidos na nota fiscal apresentada para prosseguir nos tramites de liquidação/pagamento.

10.1.2. A discriminação dos bens efetivamente entregues deverá ser reproduzida na nota fiscal apresentada para efeito de pagamento, a qual deverá ser encaminhada para o e-mail nf@cpb.org.br.

10.1.3. O não envio da nota fiscal para o e-mail nf@cpb.org.br poderá ocasionar atrasos nos tramites de liquidação/pagamento.

10.1.4. No caso de constatação de erros ou irregularidades no documento fiscal ou ainda a ausência de documentação, ocorrendo a necessidade de providências complementares por parte da contratada, a fluência do prazo de pagamento será interrompida, reiniciando a contagem a partir da data em que estas forem cumpridas.

10.2. O pagamento será efetuado por crédito em conta corrente, de titularidade da empresa e o emissor da nota fiscal, vinculada ao CNPJ.

10.3. Quaisquer pagamentos não isentarão a Contratada das responsabilidades contratuais, nem implicarão na aceitação do fornecimento relacionados e descritos no anexo I.

10.4. A Contratada fica condicionada à apresentação dos documentos a seguir para a efetivação do pagamento:

10.4.1. A Nota Fiscal deverá conter também a identificação da Ordem de Início do fornecimento, quando cabível, e o Número do Contrato;

10.4.1.1. Na hipótese de existir Nota de Retificação e/ou Nota Suplementar de Ordem de início ou Termo Assinado, cópia(s) desses(s) deverá(ão) acompanhar os demais documentos citados.

10.4.2. Regularidade Fiscal

a) Comprovante de Inscrição e de Situação Cadastral de Pessoa Jurídica no site do Ministério da Fazenda;

b) Certidão de regularidade perante o FGTS;

c) Certidão Negativa de Débitos Trabalhistas;

d) Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União;

e) Certidão de Regularidade para com as Fazendas Estadual e Municipal da sede ou domicílio da licitante, caso não seja cadastrada no Município de São Paulo, apresentar declaração firmada pelo seu representante legal/procurador, conforme anexo III.

10.5. O CNPJ da documentação fiscal deverá ser o mesmo da proposta de preço apresentada no respectivo procedimento licitatório, sob pena de rescisão contratual;

10.6. O CPB poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela empresa CONTRATADA, nos termos deste Edital e seus anexos.

10.7. Caso a CONTRATADA deixe de manter as condições exigidas para sua habilitação no certame, o presente ajuste poderá ser rescindido e, cumulativamente, será aplicada multa de até 30% sobre o valor do contrato ou da parcela vincenda.

10.8. Nenhum pagamento será efetuado na integralidade enquanto houver pendência de liquidação de obrigação financeira ou contratual em virtude de penalidade aplicada.

10.9. Previamente ao pagamento, a Contratante poderá realizar consulta aos órgãos competentes para ratificar a situação de regularidade da Contratada relativamente às condições de habilitação exigidas.

10.10. Fica ressalvada qualquer alteração futura por parte do Comitê Paralímpico Brasileiro, quanto às normas referentes a pagamento dos fornecedores, mediante prévio comunicado.

10.11. Quaisquer pagamentos não isentarão a Contratada das responsabilidades contratuais, nem implicarão na aceitação dos itens descritos no anexo I.

11. DA CONTRATAÇÃO

11.1. A contratação decorrente deste certame licitatório será formalizada mediante a assinatura de termo de contrato.

11.1.1. Se, por ocasião da celebração do contrato, algum dos documentos apresentados pela adjudicatária para fins de comprovação da regularidade fiscal e trabalhista estiverem com o prazo de validade expirado, o CPB verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando ao expediente os documentos comprobatórios, salvo impossibilidade devidamente justificada.

11.1.2. Se não for possível atualizar os documentos referidos no item 10.1.1 por meio eletrônico hábil de informações, a adjudicatária será notificada para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em plena vigência, sob pena de a contratação não se realizar.

11.1.3. Com a finalidade de verificar o eventual descumprimento pelo licitante das condições de participação previstas no item 2.2 deste Edital serão consultados, previamente à celebração da contratação, o Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções (http://www.esancoes.sp.gov.br), e Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS (http://www.portaltransparencia.gov.br/ceis)";

11.1.4. Constituem, igualmente, condições para a celebração do contrato:

a) a indicação formal de fiscal encarregado de representar a adjudicatária com exclusividade perante o contratante, bem como o responsável técnico operacional para receber as demandas do CPB;

b) a apresentação do(s) documento(s) que a adjudicatária, à época do certame licitatório, houver se comprometido a exibir antes da celebração do contrato por meio de declaração específica.

11.1.5. A não assinatura do contrato, a ausência de envio de confirmação de recebimento dentro do prazo indicado no item 11.2 importará na recusa à contratação, sujeita à aplicação das sanções cabíveis.

11.2. No prazo de 5 (cinco) dias corridos contados da data da convocação, a adjudicatária deverá comparecer perante a Contratante para assinatura do contrato.

11.2.1. O prazo indicado no item 11.2 poderá ser prorrogado por igual período, mediante solicitação justificada do interessado, desde que aceita pelo CPB.

11.2.2. O não comparecimento do fornecedor para assinatura do contrato, quando solicitado, assim como a ausência de envio de confirmação de recebimento dentro do prazo indicado no item 11.2 importarão na recusa à contratação, sujeita à aplicação das sanções cabíveis.

11.3. As demais licitantes classificadas serão convocadas para participar de nova sessão pública do pregão, com vistas à celebração do contrato, quando a adjudicatária:

11.3.1. Deixar de comprovar sua regularidade fiscal e trabalhista;

11.3.2. For convocada dentro do prazo de validade de sua proposta e não apresentar a situação regular;

11.3.3. Recusar a contratação;

11.3.4. For proibida de participar desta licitação, nos termos do item 2.6 deste Edital.

11.4. A nova sessão de que trata o item 11.3 será realizada em prazo não inferior a 03 (três) dias úteis contados da publicação do aviso no Diário Oficial da União e/ou nos sítios eletrônicos: www.cpb.org.br e www.licitacoes-e.com.br.

11.5. O contrato, quando cabível, deverá ser assinada por representante legal, diretor ou sócio da empresa, com apresentação, conforme o caso e respectivamente, de procuração ou contrato social, acompanhados de documento de identificação.

11.6. É facultado ao CPB, quando o convocado não formalizar o ajuste no prazo e condições estabelecidos, sem embargo da aplicação das penalidades cabíveis, convocar as licitantes classificadas remanescentes, na ordem de classificação de cada lote, para, querendo, fazê-lo em igual prazo, nas mesmas condições propostas pela empresa adjudicatária.

11.7. Caso a microempresa ou empresa de pequeno porte, mais bem classificada, que tenha se sagrado vencedora no preço, com o benefício do empate ficto (§ 2º do artigo 44 da Lei Complementar 123/06), não seja ao final contratada, poderão ser convocadas as remanescentes que por ventura se enquadra na mesma hipótese de empate ficto, na ordem classificatória, para o exercício do mesmo direito.

11.7.1. Os documentos mencionados nesta cláusula deverão ser apresentados em formato eletrônico de acordo com as normas da legislação vigente ou no original, com prazo de validade em vigor na data da apresentação e serão

retidos para oportuna juntada no processo administrativo pertinente à contratação.

12. DAS SANÇÕES

12.1. Além das sanções previstas na cláusula nona, da Minuta do Contrato, Anexo IX, também poderão ser aplicadas à CONTRATADA as sanções previstas na Lei Federal nº 14.133/2021 e demais normas pertinentes, assim como as penalidades abaixo elencadas, sendo-lhe sempre assegurada o contraditório e a ampla defesa.

12.2. Ocorrendo recusa em assinar o contrato e/ou fornecer o objeto, dentro do prazo estabelecido neste Edital, sem justificativa aceita pelo CPB, garantido o direito ao contraditório e à ampla defesa mediante prévia notificação, serão aplicadas:

12.2.1. Multa no valor de 30% (trinta por cento) do valor do ajuste se firmado fosse;

12.2.2. Pena de suspensão temporária do direito de licitar e contratar com o Comitê Paralímpico Brasileiro pelo prazo de até 2 (dois) anos.

12.3. A licitante que ensejar o retardamento da execução do certame, inclusive em razão de comportamento inadequado de seus representantes, der causa a tumultos durante a sessão pública de pregão, deixar de entregar ou apresentar documentação falsa exigida neste edital, não mantiver a proposta/lance, comportar-se de modo inidôneo, fizer declaração falsa, garantido o direito ao contraditório e à ampla defesa mediante prévia notificação, serão aplicadas as penalidades referidas nos subitens 12.2.1 e 12.2.2, a critério do CPB.

12.4. As sanções são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

12.5. O prazo para pagamento da multa será de 05 (cinco) dias úteis a contar da intimação da empresa apenada. A critério do CPB e em sendo possível, o valor devido será descontado da importância que ela tenha a receber do CPB.

12.6. Em caso de inadimplemento da multa imposta, o valor será reajustado pelo índice IPCA e sofrerá incidência de juros de mora de 1% ao mês.

12.7. São aplicáveis à presente licitação, inclusive, as sanções penais estabelecidas na Lei Federal nº 14.133/21, bem como as disposições do Código de Defesa do Consumidor.

12.8. Quando da execução do objeto desta licitação, a empresa estará sujeita às penalidades previstas no Regulamento de Aquisições e Contratos, instituído pela resolução CPB nº 01 de abril de 2023, nas proporções e condições descritas na Minuta do Contrato, Anexo IX deste Edital.

13. DAS OBRIGAÇÕES DA CONTRATADA

13.1. Além das obrigações constantes do Anexo I do Edital, cabe a CONTRATADA as obrigações previstas na Minuta do Contrato, Anexo IX do Edital.

14. DAS OBRIGAÇÕES DA CONTRATANTE

14.1. Além das obrigações constantes do Anexo I do Edital, cabe a CONTRATANTE as obrigações previstas na Minuta do Contrato, Anexo IX do Edital.

15. DA GARANTIA CONTRATUAL

15.1. Não será exigida a prestação de garantia para a contratação resultante desta licitação.

16. DAS DISPOSIÇÕES FINAIS

16.1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, da transparência, respeitada a igualdade de oportunidade entre as licitantes, desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

16.2. Das sessões públicas de processamento do Pregão Eletrônico serão lavradas atas circunstanciadas, a serem assinadas pelo Pregoeiro e pela equipe de apoio.

16.3. O sistema manterá sigilo quanto à identidade das licitantes: para o Pregoeiro, até a etapa de negociação com o autor da melhor oferta e para os demais participantes, até a etapa de habilitação.

16.4. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos à publicação, serão divulgados nos sítios eletrônicos www.cpb.org.br e www.licitacoes-e.com.br.

16.5. Até 3 (três) dias úteis anteriores à data fixada para abertura da sessão pública, qualquer pessoa poderá, exclusivamente, por meio do sistema eletrônico, solicitar esclarecimentos, informações ou impugnar o ato convocatório do Pregão Eletrônico, conforme Art. 164, da Lei Federal 14.133/21.

16.6. A impugnação, assim como os pedidos de esclarecimentos e informações, será formulada, exclusivamente por meio do sistema eletrônico, www.licitacoes-e.com.br em campo próprio do sistema. Caso o licitante não consiga incluir no sistema, por motivo justificado, este deverá encaminhar o esclarecimento / impugnação, nos prazos citados acima, para o e-mail pregao@cpb.org.br.

16.6.1. Caso os pedidos de esclarecimentos / impugnação sejam realizados via e-mail, o pregoeiro disponibilizará, no campo "MENSAGENS" do sistema LICITACOES-

E, o pedido e a resposta referente ao questionamento do licitante, para ciência dos demais licitantes.

16.7. As impugnações serão decididas pela autoridade Competente e respondidas pelo subscritor do Edital e os esclarecimentos e informações prestados pelo pregoeiro, no prazo de até 1 (um) dia útil, anterior à data fixada para abertura da sessão pública. Após respondidos, qualquer alteração / acréscimo de informação que venha a surgir de algum esclarecimento, automaticamente passará a fazer parte do Edital do Certame e deverá ser conhecido pelos demais licitantes.

16.8. Acolhida a impugnação contra o ato convocatório, será designada nova data para realização da sessão pública.

16.9. Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro, e as questões relativas ao sistema, pelo suporte do "Sistema do LICITACOES-E".

16.10. Fica a licitante ciente de que a apresentação da proposta implica a aceitação de todas as condições deste Edital e seus anexos, não podendo invocar qualquer desconhecimento dos termos do edital ou das disposições legais aplicáveis a espécie, como elemento impeditivo da formulação de sua proposta ou do perfeito cumprimento do ajuste.

16.11. As licitantes assumem todos os custos de preparação e apresentação de suas propostas e o CPB não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

16.12. As licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do certame.

16.13. O ajuste, suas alterações e rescisão obedecerão à Lei Federal nº 14.133/2021, demais normas complementares e disposições deste Edital, aplicáveis à execução das avenças e especialmente os casos omissos.

16.14. O CPB poderá, a qualquer tempo, motivadamente, revogar ou anular, no todo ou em parte a licitação, sem que tenham as licitantes direito a qualquer indenização, observado o disposto no artigo 71 da Lei Federal nº 14.133/2021.

16.15. Com base no artigo 64, da Lei Federal nº 14.133/2021, é facultada à Comissão Julgadora, em qualquer fase da licitação, promover diligência destinada a esclarecer ou a complementar a instrução do processo.

16.16. Os casos omissos e as dúvidas surgidas serão resolvidos pela Comissão de Licitação, ouvida, se for o caso, as Unidades competentes.

16.17. Integrarão o ajuste a ser firmado, para todos os fins, a proposta da CONTRATADA, a Ata de Julgamento da licitação, por conter os valores obtidos ao final da etapa de lances, a proposta readequada com as reduções obtidas após a Licitação e o Edital da Licitação, com seus anexos, que o precedeu.

16.18. Nenhuma tolerância das partes quanto à falta de cumprimento de quaisquer das cláusulas do ajuste poderá ser entendida como aceitação, novação ou precedente.

16.19. Fica ressalvada a possibilidade de alteração das condições contratuais em face da superveniência de normas federais disciplinando a matéria.

16.20. Na contagem dos prazos estabelecidos neste edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente do CPB.

16.21. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do certame, o Sistema eletrônico poderá permanecer acessível aos licitantes para recepção dos lances, retomando o Pregoeiro, quando possível, sua atuação no Pregão, sem prejuízos dos atos realizados. Quando a desconexão persistir por tempo superior a 15 (quinze) minutos, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa aos licitantes.

16.22. A presente licitação não importa necessariamente em contratação, podendo o Comitê Paralímpico Brasileiro revogá-la, no todo ou em parte, por razões de interesse público, derivada de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação, mediante ato escrito e fundamentado, disponibilizado no Sistema para conhecimento dos licitantes da licitação.

16.23. As decisões referentes a este processo licitatório serão comunicadas através do Sistema Eletrônico de Compras, na página correspondente à licitação, e poderão ser estendidas aos licitantes por qualquer outro meio de comunicação ou, ainda, mediante publicação no Diário Oficial da União.

16.24. Fica desde logo eleito o Foro do Município de São Paulo para dirimir quaisquer controvérsias decorrentes do presente certame.

16.25. Integram o presente Edital:

Anexo I	**Termo de Referência;**
Anexo II	**Modelo de Planilha de Proposta;**
Anexo III	**Modelo de Declaração que nada deve à Fazenda Municipal;**
Anexo IV	**Modelo de Declaração: Constituição Federal – artigo 7º, não há impedimentos em licitar; enquadramento como ME/EPP e Reserva de Cargos;**
Anexo V	**Modelo de Declaração – Lei anticorrupção;**
Anexo VI	**Cadastro de Fornecedor;**
Anexo VII	**Questionário de Due Diligence de Integridade;**
Anexo VIII	**Minuta do Contrato.**

São Paulo, 24 de julho de 2024.

Beatriz Martins
Pregoeira
Comitê Paralímpico Brasileiro

ANEXO I
TERMO DE REFERÊNCIA

PROCESSO Nº 0696/2024
CÓDIGO DO ÓRGÃO XXXXXXXX
MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

1. JUSTIFICATIVA DA CONTRATAÇÃO

1.1. Com o aumento das ameaças cibernéticas e a sofisticação dos ataques, investir em medidas de segurança robustas tornou-se uma prioridade para empresas. Nesse contexto, tanto o Firewall de Próxima Geração (NGFW) quanto o antivírus desempenham papéis cruciais na proteção contra ameaças virtuais. Destes serviços, podemos destacar a viabilidade para utilização de toda a conectividade de rede – acesso à internet – de modo seguro e controlado, aplicando regras, filtros e bloqueios para proteção contra ataques, roubo de dados e demais ameaças cibernéticas.
O número informado de 600 licenças de antivírus se dá pela quantidade de usuários Instituição.
Verifica-se ainda, para melhor entendimento e adoção das melhores práticas a necessidade de treinamento e acompanhamento para os responsáveis de TI.

2. DO OBJETO

2.1. Fornecimento de modelos idênticos de Firewall e licenças de antivírus para notebooks, desktops, dispositivos móveis, servidores físicos e virtuais, por período de 12 meses, a serem entregues no Comitê Paralímpico Brasileiro (CPB), localizado na cidade de São Paulo – SP, Rodovia dos Imigrantes, KM11,5, CEP 04.329-000. O Contratante poderá solicitar a quantidade que desejar, sob demanda, até o limite máximo estipulado neste edital. Visando garantir 100% da integração da solução, o Firewall e o Antivírus devem ser do mesmo fabricante.

Referência	Quantidade máxima	Valor Unitário	Valor total
Firewall	2		
Licença de antivírus	600		
Implementação e treinamento	Único		

3. CARACTERÍSTICAS GERAIS

3.1. A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

3.2. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

3.3. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

3.4. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

3.5. Todos os componentes devem ser próprios para montagem em rack "19" e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

3.6. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

3.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

4. CAPACIDADE E QUANTIDADES

4.1. **SOLUÇÃO EM APPLIANCE DE SEGURANÇA DE PERÍMETRO DE PRÓXIMA GERAÇÃO**:

4.1.1. Throughput de, no mínimo, 6,6 (seis vírgula seis) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero;

4.1.2. Suporte a, no mínimo, 7M (sete milhões) de conexões simultâneas;

4.1.3. Suporte a, no mínimo, 250.000 (duzentos e cinquenta mil) novas conexões por segundo;

4.1.4. Throughput de, no mínimo, 28 (vinte e oito) Gbps, no mínimo, para conexões VPN;

4.1.5. Suportar no mínimo, a criação de 20 instancias/contextos virtuais de firewall;

4.1.6. Deve suportar a performance considerando as funcionalidades de Next Generation firewall de 19 (dezenove) Gbps;

4.1.7. Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;

4.1.8. Fonte de alimentação redundante e hot-swappable;

4.1.9. Througupt de no mínimo, 30 (trinta) Gbps de IPS;

4.1.10. Deve possuir no mínimo 32 GB de memória RAM;

4.1.11. No mínimo, 08 (oito) interfaces de rede 10Gbps SFP+;

4.1.12. No mínimo, 08 (oito) interfaces de rede 10/100/1000 base-T;

4.1.13. Possuir 1 (uma) interface de rede dedicada para sincronismo;

4.1.14. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

4.1.15. Possuir 1 (uma) interface do tipo console ou similar;

4.1.16. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.

4.1.17. Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;

4.1.18. Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes com no mínimo 480 GB de capacidade de armazenamento para o Sistema Operacional.

4.1.19. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.20. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.

4.1.21. Solução de suportar Dual stack ipv4/ipv6 e NAT64.

4.1.22. Suportar configurar IPv6 em Dual Stack em uma interface Bond/Agregação, essa configuração também pode ser configurada em uma Sub-interface de Bond/Agregação;

4.1.23. Deve suportar NAT64 e NAT46;

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

4.1.25. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;

4.1.26. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

4.1.27. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

4.1.28. Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;

4.1.29. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;

5. FUNCIONALIDADE DE FIREWALL

5.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

5.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

5.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

5.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

5.5. Realizar upgrade via SCP, SFTP e https via interface WEB.

5.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

5.7. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

5.8. Deverá suportar VXLAN;

5.9. Deve suportar os seguintes tipos de NAT:

5.10. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

5.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

5.12. As regras de NAT devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;

5.13. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

5.14. Enviar logs para sistemas de monitoração externos, simultaneamente;

5.15. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

5.16. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.

5.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

5.18. Suportar OSPF graceful restart;

5.19. Deve suportar roteamento ECMP (equal cost multi-path);

5.20. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultanea usando os seguintes parâmetros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

5.21. Autenticação integrada via Kerberos.

5.22. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

5.23. As regras Firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;

5.24. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

5.25. A solução deve ter a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

5.26. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

5.27. Deve possuir mecanismo de ativação de validada da regra com período customizado;

5.28. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet.

5.29. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

5.30. Deve permitir a configuração do tempo de checagem para cada um dos links.

6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

6.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

6.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

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

6.4. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

6.5. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

6.6. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

6.7. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

6.8. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

6.9. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

6.10. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

6.11. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

6.12. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

6.13. 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;

6.14. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

6.15. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

6.16. Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação princial e/ou as suas sub-categorias. Quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo

que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de applicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

6.17. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicamção;

6.18. Atualizar a base de assinaturas de aplicações automaticamente;

6.19. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

6.20. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

6.21. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

6.22. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

6.23. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

6.24. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

6.25. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

6.26. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

6.27. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

6.28. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

6.29. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

6.30. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

6.31. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

6.32. Suportar a criação de categorias de URLs customizadas;

6.33. Suportar a exclusão de URLs do bloqueio, por categoria;

6.34. Permitir a customização de página de bloqueio;

6.35. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

6.36. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

6.37. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

7. FUNCIONALIDADE DE FILTRO DE DADOS

7.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

a) • PCI - credit card numbers
b) • HIPAA - Medical Records Number - MRN
c) • International Bank Account Numbers - IBAN
d) • Source Code - JAVA
e) • U.S. Social Security Numbers - According to SSA
f) • Salary Survey Terms
g) • Viewer File - PDF
h) • Executable file
i) • Database file
j) • Document file

k) • Presentation file
l) • Spreadsheet file

7.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

7.3. A solução de controle de dados deve premir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

7.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

8. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

8.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

8.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

8.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

8.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

8.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

8.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

8.7. Detectar e bloquear a origem de portscans;

8.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

8.9. Possuir assinaturas para bloqueio de ataques de buffer overflow;

8.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

8.11. Suportar bloqueio de arquivos por tipo;

8.12. Identificar e bloquear comunicação com botnets;

8.13. Deve suportar referência cruzada com CVE;

8.14. Em cada proteção de segurança, deve estar incluso informações como:

I. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;
II. Severidade;
III. Tipo de ação a ser executada.

8.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

8.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

8.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

8.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

8.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

8.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

8.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

8.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

8.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção deve ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

8.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

8.24. A solução deverá possuir pelo menos dois perfis préconfigurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

8.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

8.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

8.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

8.28. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

8.29. A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

8.30. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

8.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

8.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

8.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

8.34. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

8.35. Os eventos devem identificar o país de onde partiu a ameaça;

8.36. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

8.37. Suportar rastreamento de vírus em arquivos pdf;

8.38. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

8.39. Possuir a capacidade de prevenção de ameaças não conhecidas;

8.40. Em caso de falha no mecanismo de inspeção do Anti-Virus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

8.41. A solução de Anti-virus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

8.42. A solução Antivirus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

8.43. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

8.45. A solução deverá possuir mecanismo de "machine learning" para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorith) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

8.46. A solução deverá possuir mecanismo de "machine learning" para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

8.47. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

8.48. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

8.49. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

8.50. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

9. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

9.1. Suportar a criação de políticas de QoS por:

9.2. Endereço de origem, endereço de destino e por porta;

9.3. O QoS deve possibilitar a definição de classes por:

9.4. Banda garantida, banda máxima e fila de prioridade;

9.5. Disponibilizar estatísticas em tempo real para classes de QoS;

10. FUNCIONALIDADES DE VPN

10.1. Suportar VPN Site-to-Site e Cliente-To-Site;

10.2. Suportar IPSec VPN;

10.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

10.4. Suportar SSL VPN;

10.5. A VPN IPSEc deve suportar:

10.5.1. 3DES, Autenticação MD5, SHA-1, SHA-384, AES-XCBC, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

10.6. A VPN SSL deve suportar:

10.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

10.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

10.6.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

10.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

10.6.5. Atribuição de DNS nos clientes remotos de VPN;

10.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

10.6.7. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

10.6.8. A solução deve permitir bloquear o acesso do usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.

10.6.9. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

10.6.10. A solução deve permitir a integração da ferramenta com provedores de identidade, através de SAML, para autenticação dos usuários remotos conectados via VPN;

10.6.11. Suportar leitura e verificação de CRL (certificate revocation list);'

10.6.12. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

10.6.13. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

11. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

11.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

11.2. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

11.3. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

11.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

11.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

11.6. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

11.7. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

11.8. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

11.9. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

11.10. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

11.11. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

11.12. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

11.13. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

11.14. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

11.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

11.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

11.17. A solução deve suportar inspeção para o protocolo SMBv3;

11.18. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

11.19. A solução deve possuir engine de inspeção a nivel de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

11.20. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

11.21. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

11.22. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

11.23. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

11.24. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

11.25. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

11.26. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

11.27. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing ;

11.28. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

11.29. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

11.29.1. Número de arquivos emulados;
11.29.2. Número de arquivos com malware.

11.30. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

11.31. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

11.31.1. O tamanho máximo do arquivo emulado seja excedido;
11.31.2. O tempo máximo de emulação seja excedido.

12. MÓDULO DE GERÊNCIA

12.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

12.2. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

12.3. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

12.4. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

12.5. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

12.6. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

12.7. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

12.8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

12.9. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

12.10. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

12.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

12.12. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

12.13. Suportar backup das configurações e rollback de configuração para a última configuração salva;

12.14. Suportar validação de regras antes da aplicação;

12.15. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

12.16. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

12.17. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

12.18. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

12.19. Permitir a criação de certificados digitais para autenticação de usuários;

12.20. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);

12.21. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

12.22. A solução deve permitir a integração da ferramenta com provedores de identidade para authenticação dos administradores da solução via SAML 2.0;

12.23. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

12.23.1. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

12.23.2. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.

12.24. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

12.25. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

12.26. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

12.27. Deve ser possível exportar os logs em CSV ou TXT;

12.28. A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

12.29. A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

12.30. A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

12.31. O visualizador de log deve ter um recurso de pesquisa de texto livre;

12.32. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

12.33. Possibilitar rotação do log;

12.34. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

12.34.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, 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-Malware), de rede vinculadas a este tráfego;

12.35. Deve permitir a criação de relatórios personalizados;

12.36. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

12.37. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI);

12.38. Possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

12.39. Deve consolidar logs e relatórios de todos os dispositivos administrados;

12.40. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

12.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

12.42. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

12.43. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo.

12.43.1. ISO 27001 e ISO 27002;
12.43.2. PCI-DSS;
12.43.3. NIST 800-41
12.43.4. GDPR (base da norma LGPD);

12.44. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição irá seguir. Não sendo permitido licenciamento mensalizado “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.

12.45. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.

12.46. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

12.47. Permitir a customização do padrão regulatório da própria instituição;

12.48. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

12.49. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

12.50. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;

12.51. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

12.52. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

12.53. Possuir alertas de políticas e as potenciais violações de conformidade;

12.54. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

12.55. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

12.56. Permitir que os relatórios possam ser salvos, enviados e impressos;

12.57. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc.;

12.58. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

12.58.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
12.58.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

12.59. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

12.60. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

12.61. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

12.62. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

12.63. Criar certificados digitais para acesso dos usuários VPN;

12.64. Criar certificados digitais para VPNs Site-to-Site;

12.65. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

12.66. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

12.67. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

12.68. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.

12.69. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

12.70. A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino do logs na mesma tela de pesquisa.

12.71. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

12.72. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

12.73. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

12.74. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

12.75. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

12.76. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

12.77. A solução deve ser capaz de personalizar e criar regras de correlação;

12.78. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

12.79. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

13. PROTEÇÃO CONTRA AMEAÇAS PERSISTENTES AVANÇADAS (APT) PARA ESTAÇÃO DE TRABALHO

13.1. CARACTERÍSTICAS GERAIS

13.2. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

13.3. A solução de proteção avançada para notebooks, desktops e servidores consiste em um agente de segurança que será responsável pela análise de arquivos e comportamentos no sistema operacional do computador do usuário final ou servidor a fim de bloquear qualquer tipo de ameaça conhecida e vulnerabilidade de dia-zero.

13.4. Deve escanear arquivos e identificar infecções baseado em características comportamentais dos vírus;

13.5. Deve escanear arquivos quando eles forem acessados, executados, permitindo detecção imediata e tratamento por qualquer ameaça;

13.6. Deve permitir executar uma análise detalhada de cada arquivo conforme selecionado pelo usuário;

13.7. Deve permitir especificar diretórios e extensões de arquivos para que sejam excluídos da análise de vírus;

13.8. Deve checar as áreas mais comuns do sistema de arquivos e a registry do sistema operacional em busca de ameaças avançadas;

13.9. Deve possuir as seguintes opções de remediação:

13.10. Reparar;

13.11. Quarentenar;

13.12. Apagar;

13.13. Deve permitir ser gerenciado através de console unificada para gerenciamento centralizado de políticas e logs.

13.14. Deve identificar automaticamente o ponto de entrada do malware e o seu impacto para a organização;

13.15. A solução deve suportar os sistemas operacionais com versões mínimas de Windows 7 e Windows Server 2008 R2.

13.16. Deve gerar automaticamente relatório completo da execução do malware utilizando técnicas contidas no MITRE Framework;

13.17. Deve detectar ataques desconhecidos e de dia-zero. Arquivos copiados ou que tenha sido efetuado download devem ser enviados para emulação (sandboxing) em ambiente controlado a fim de detectar ataques de dia-zero;

13.18. Deve bloquear ataques independentemente se o vetor de distribuição é baseado na web, email ou mídia removível;

13.19. Deve detectar e bloquear comunicações com servidores de comando e controle (C&C) para impedir vazamento de dados mesmo quando conectado/trabalhando remotamente. Deve permitir a quarentena de sistemas infectados para evitar que o malware se espalhe;

13.20. Deve possuir funcionalidade de análise forense de incidente, provendo uma visão completa do fluxo do ataque, causa raiz, impacto no negócio e o ponto de entrada do malware para agilizar as ações de remediação;

13.21. O Endpoint deve ser integrado ao Antivírus (agente único e gerenciamento), que fornece uma forte proteção de primeira linha estática e dinâmica usando assinaturas e análise comportamental.

13.22. Deve suportar emulação Threat sandbox, que inclui tecnologias de detecção para identificar malware desconhecido para o qual a assinaturas. Isso é realizado combinando recursos avançados de aprendizado de máquina, análise comportamental dinâmica de SO, identificando comportamentos suspeitos e mal-intencionados, táticas de hacking e técnicas de engenharia social, analisando as comunicações C&C durante a análise do sandbox e muito mais. O malware detectado é impedido de baixar (a sessão de download é interceptada pelo Endpoint). Se o malware já estiver na máquina, ele será colocado em quarentena.

13.23. A solução pode ser configurada para enviar arquivos para emulação no dispositivo de sandbox local e na nuvem.

13.24. Deve possuir prevenção contra malware de dia zero, realizando a extração de ameaças fornecendo arquivos higienizados para os usuários;

13.25. O produto deve suportar no mínimo dois modos básicos de higienização de arquivos:

13.26. Manter tipo de arquivo - entregar o arquivo em seu formato original, removendo qualquer conteúdo ativo, como macros;

13.27. Converter para PDF - os arquivos entregues aos usuários são convertidos para o formato PDF, uma transformação praticamente impossível para qualquer malware sobreviver. Dessa forma os usuários podem obter acesso auto-suficiente ao arquivo original, se tal acesso for necessário. O acesso é garantido apenas se o arquivo for limpo pelo mecanismo de detecção de emulação de ameaças.

13.28. O endpoint deve fornecer a capacidade de ativar / desativar granularmente cada funcionalidade, que serve como um meio para isolar qualquer interferência com outros aplicativos. Além das ferramentas de solução de problemas padrão, as informações de forense podem ajudar na identificação de tais interferências;

13.29. Deve ser capaz de efetuar roll-back de mudanças no registro do Windows e alterações no sistema de arquivos em caso de alteração a arquivos infectados;

13.30. Deve possuir extensão para navegador Internet, Google Chrome e Internet Explorer, para prevenir contra ameaças avançadas de dia-zero e extração de conteúdos maliciosos para os downloads efetuados via web pelos usuários;

13.31. Deve proteger os dados forenses armazenados na estação de trabalho (Endpoint) contra acessos não autorizados ou outro tipo de tentativa de manipulação através da estrutura segura de logs da solução;

13.32. Os clientes se comunicam apenas com servidores autorizados (ou seja, apenas IPs específicos fornecidos por um servidor autenticado) e realizam a validação do certificado do servidor (usando informações internas) para verificar se o servidor é confiável;

13.33. Deve possuir análise de campos de login e senha em caso de acesso a páginas de internet como e-mail e formulários na detecção e prevenção de sites de phishing;

13.34. Deve possuir mecanismo de proteção para evitar que o usuário use credenciais corporativas em sites não corporativos.

13.35. A solução deve ser capaz de fazer remediação de forma automatizada, sem a necessidade da intervenção do usuário;

13.36. A solução deverá detectar e bloquear tem tempo real qualquer ação maliciosa ao sistema operacional que venha através de download de arquivos na Web, copia através de um drive externo, sites de phishing e até mesmo mecanismos de criptografia de arquivos como o Ransomware. Sendo que a solução deve possuir mecanismos de restauração dos arquivos no momento que é detectado e bloqueado o Ransomware, ou seja, não permitindo o sequestramento de informações.

13.37. A solução deverá detectar e bloquear ameaças em download ou através de movimento lateral (cópia de arquivos) em qualquer extensão Microsoft Office, sendo ela capaz de detectar qualquer tipo de executável que tente criptografar os arquivos do computador do usuário.

13.38. A solução deverá detectar e bloquear malwares dia zero no momento do download e cópia através de drive externo. Deve prevenir e remediar de forma automática ataques evasivos de Ransonware, baseado em análise comportamental;

13.39. Deve reverter as ações do Ransonware, restaurando os dados corporativos automaticamente, garantindo proteção contra criptografia dos dados;

13.40. Possuir tecnologia que não seja baseada em assinaturas, garantindo seu funcionamento tanto de forma online quanto offline;

13.41. Deve permitir que os agentes obtenham atualizações de assinaturas através de um ponto local, sem uma conexão com o serviço de gerenciamento.

13.42. Deve implementar, através de análise dinâmica e heurística, proteção em tempo real contra sites conhecidos e desconhecidos de phishing;

13.43. Deve detectar, através de análise estática e heurística, elementos suspeitos em sites que solicitem credenciais dos usuários;

13.44. Deve detectar e prevenir a reutilização de credenciais corporativas em sites externos;

13.45. Deve ser suportar o monitoramento do Log de Eventos do Windows para analisar eventos de malware de fornecedores de antivírus de terceiros.

13.46. Deve ser capaz de realizar ações com base no Log de Eventos do Windows, como:

13.47. Analisar ataques

13.48. Encerrar processos

13.49. Excluir ou colocar arquivos em quarentena

13.50. Deve possuir processo de análise forense automático de incidentes, disponibilizando as seguintes informações sobre o ataque:

13.51. Eventos Maliciosos;

13.52. Ponto de entrada do malware;

13.53. Escopo dos danos causados;

13.54. Máquinas infectadas;

13.55. Deverá ser capaz de realizar importação customizada de Indicadores de Comprometimentos (IOC) externos;

14. <u>Criptografia de disco, mídias removíveis e controle de periféricos</u>

14.1. A solução deverá possibilitar a criptografia do disco para Windows/MacOS e de mídias removíveis como dispositivos de armazenamento USB e unidades de disco externas, a fim de garantir que apenas usuários autorizados, possam ter acesso aos dados armazenados nestes dispositivos;

14.2. Para Windows, a solução deve possibilitar a escolha de criptografia do disco utilizando o Bitlocker ou ferramenta de criptografia proprietária do fabricante;

14.3. A ferramenta de criptografia proprietária deve utilizar ao menos os seguintes algoritmos de criptografia:

14.4. AES-CBC 256 bit;

14.5. XTS-AES 128 bit;

14.6. XTS-AES 256 bit;

14.7. Para MacOS deverá permitir a criptografia do disco utilizando o File Vault;

14.8. Possuir a capacidade de criar políticas granulares que permitem definir em quais máquinas serão aplicadas a criptografia de disco;

14.9. Deverá possibilitar a criptografia do disco inteiro ou apenas do espaço utilizado;

14.10. Permitir escolher entre criptografia de todos os discos ou apenas do disco onde foi instalado o sistema operacional;

14.11. A solução deve possibilitar a criptografia de discos ocultos;

14.12. Deverá permitir que o usuário se autentique antes do carregamento do sistema operacional (pre-boot) para evitar acesso não autorizado ao SO;

14.13. Permitir que o administrador possa desativar a proteção de pré-inicialização temporariamente, por exemplo, para manutenção.

14.14. Utilizar o procedimento de desafio/resposta para que o administrador possa ajudar remotamente o usuário que possui criptografia de disco em seu computador a recuperar seu acesso.

14.15. Com relação a criptografia de mídia removível, a solução deverá:

14.16. Realizar um scan em busca de malwares na mídia removível antes de autorizar o uso da mesma;

14.17. Sugerir que o usuário realize a criptografia mesmo quando configurado como não mandatório;

14.18. Permitir configurar quantos por cento de espaço da mídia removível será utilizado para criptografia;

14.19. Possibilitar a segregação de dados corporativos de não corporativos, garantindo que os dados corporativos estejam criptografados e que só possam ser acessados por pessoas autorizadas;

14.20. Garantir acesso ao dado criptografado através de senha caso o usuário esteja em uma máquina não gerenciada;

14.21. Permitir com que o usuário recupere a senha através de um auxílio remoto do administrador.

14.22. Caso o administrador não deseje habilitar o recurso de criptografia de mídia removível, a solução deve ser capaz de bloquear a porta USB para impedir a conexão de um dispositivo externo.

14.23. Além da porta USB, a solução deverá permitir o controle (permitir ou bloquear) de periféricos como mouse, teclado e impressoras e até mesmo dispositivos que se conectem via bluetooth.

14.24. Assim como para a criptografia, a solução deve possuir a capacidade de criar políticas granulares que permitem definir em quais máquinas serão aplicadas as políticas de criptografia de mídia removível e/ou proteção de portas.

15. GERENCIAMENTO CENTRALIZADO DE POLÍTICAS DE SEGURANÇA, LOGS E RELATÓRIOS:

15.1. O Software de Gerência deve ser capaz de gerenciar todos os endpoint de Segurança de forma centralizada, possibilitando a concentração dos Logs e emissão de relatórios.

15.2. A gerência dos endpoints deve ser realizada através de console própria ou através de interface web (HTTPS).

15.3. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos.

15.4. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.

15.5. Acesso avançado para monitorar e gerenciar as funções do sistema

15.6. A solução deve ter integração com o Microsoft Active Directory para identificação de usuários

15.7. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e análise dos eventos;

15.8. A solução de gerenciamento deverá ser entregue em nuvem do próprio fabricante, ou em appliance do próprio fabricante ou servidores de terceiros sendo eles listados em uma base de compatibilidade de hardware ou ambiente virtualizado;

15.9. A solução deve apresentar sumário apontando os agentes que estão instalados, em progresso ou que ainda estão pendentes;

15.10. A gerência deve apontar os agentes nos endpoints que foram violados com Segurança;

15.11. Todos os logs deverão ser referenciados com o nome do usuário devido a integração com o Active Directory.

15.12. A solução deve possuir outros módulos de Segurança onde podem ser incorporadas na mesma console de gerenciamento.

15.13. Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos

15.14. Disponibilizar recursos interativos de navegação nos eventos informados;

15.15. A solução deve possuir relatórios customizáveis onde seja possível pegar diferentes informações para montagem do relatório;

15.16. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações: bloqueio da origem, envio de snmp e envio de email;

15.17. A solução deve exportar relatórios via HTML e CSV;

15.18. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

15.19. A solução deve permitir o administrador ser capaz de atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.

15.20. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:

15.21. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

15.22. Estatísticas com comparativo de período (hora, dia e mês);

15.23. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;

15.24. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e análise dos eventos;

15.25. Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por pais.

15.26. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

15.27. Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino.

15.28. Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes.

15.29. Deve estar incluso no dashboard com horários predefinidos, diários, semanais e relatórios mensais. Incluindo:

15.29.1. Top eventos,
15.29.2. Top origem,
15.29.3. Top destinos,
15.29.4. Top Serviços,
15.29.5. Top origens e os seus principais eventos,
15.29.6. Top destinos e seus principais eventos;

15.30. Solução deve incluir relatórios de horários, diários, semanais e mensais pré-definidos. Incluindo pelo menos eventos Top origem, Top destino, Top evento, Top users, Top localidade de origem e os principais eventos relacionados em cada filtro;

15.30.1. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado.

15.30.2. A solução deve possuir pesquisa através de todos os endpoints instalados para buscar informações relacionadas a nome de processo, MD5 do arquivo, IP da rede origem, IP da rede de destino, URL, nome do arquivo, tipo do arquivo para identificação de possíveis atividades anômalas no ambiente corporativo.

15.30.3. A solução deve possuir pesquisa das principais atividades maliciosas, através de pesquisas baseadas em processos, palavras chaves ou usuário. Quando encontrado, deve ser possível incluir outras informações no campo de busca que podem ser combinadas no período determinado pelo administrador. Assim, terá ampla visibilidade da informação que foi colocado na busca em todos os endponits instalados no ambiente de produção;

15.30.4. A ferramenta deve apresentar linha do tempo com as principais atividade de rede e ameaças permitindo o administrador ter mais informações entre elas:

15.30.4.1. Detalhes da rede

15.30.4.2. Detalhe do dispositivo identificando contendo informações do usuário, computador, OS Name, OS version, Domain Name e Host MACs.

15.30.4.3. Detalhes do processo que foi identificado através da busca realizada.

15.30.4.4. Horário da atividade que foi identificada.

15.30.5. Quando identifica qualquer atividade de rede ou ameaça através da ferramenta, a solução deve permitir o administrador a realizar ações como:

15.30.5.1. Terminar processo;
15.30.5.2. Quarentenar arquivo;
15.30.5.3. Ter acesso a análise forense.

15.30.6. Deverá permitir consultas predefinidas de vulnerabilidades reais, permitindo também uma visualização do painel MITTRE&ATTACK, ajudando na identificação das técnicas de evasão baseado neste framework.

15.30.7. A solução deve agrupar ao menos as seguintes informações referentes ao gerenciamento de postura das máquinas:

15.30.7.1. Vulnerabilidades agrupadas por severidade (Crítica, importante, moderada ou Baixa);

15.30.7.2. Top softwares instalados que apresentam maior risco;

15.30.7.3. Top dispositivos vulneráveis.

15.30.8. Deverá ser possível extrair um relatório com informações das vulnerabilidades associadas aos softwares instalados nas máquinas (Gerenciamento de Postura).

16. CONDIÇÕES DE PAGAMENTO

16.1. Todo o equipamento e licença solicitada pelo contratante será pago em parcela única para período de 12 meses;

16.2. A contratante tem prazo de 30 dias corridos para pagamento após a emissão da nota fiscal.

16.3. Para emissão da nota fiscal, a Contratada deverá ter o aceite do contratante referente a ativação de todos os serviços e que não restam mais pendências

16.4. A nota fiscal deve constar apenas a quantidade solicitada pelo contratante.

17. CONDIÇÕES GERAIS

17.1. É permitido ao contratante renovar todos os serviços ou apenas parte deles.

17.2. A contratada deverá configurar toda a solução de Firewall e Antivírus conforme orientação/documentação que será repassada pelo CPB.

17.3. Deve ser realizado um treinamento da solução de Firewall e Antivírus, sendo obrigatório a apresentação de todos os recursos/funcionalidades das soluções contratadas no prazo máximo de 5 dias corridos após a implantação dos serviços

17.4. A contratada deverá ofertar, durante toda vigência do contrato, 20h mensais de suporte assistido à contratante, não cumulativas, sempre que solicitada por um canal oficial de abertura destes serviços;

17.5. Sempre que solicitado pela contratante, a contratada deverá agendar o atendimento no prazo máximo de 1 dia útil.

17.6. Casos não solucionados imediatamente devem ter o posicionamento oficial/final da fabricante no prazo máximo de 3 dias úteis.

17.7. Estes serviços devem contemplar toda a solução contratada.

17.8. Caso algum dos firewalls apresente problema, a contratante deverá substituí-lo em prazo máximo de 10 dias;

17.9. Caso seja notificado pela contratada que todos os Firewalls estão inoperantes, a contratante deverá substituir pelo menos um dos equipamentos em até 4h

17.10. A contratada deve manter, durante a vigência do contrato, backup das configurações de firewall

17.11. Prazo de entrega dos serviços solicitados pelo contratante: 30 dias corridos. Este prazo contará após a assinatura do contrato.

Danillo Vieira Nascimento / Eduardo Jesus

ANEXO II
MODELO DE PROPOSTA

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

AO COMITÊ PARALÍMPICO BRASILEIRO

A empresa ....., estabelecida à ..... inscrita no CNPJ sob nº ....., telefone nº ..... e endereço de e-mail ....., através de seu representante legal abaixo assinado, propõe assinar Termo de Contratos junto ao Comitê Paralímpico Brasileiro, em estrito cumprimento ao previsto no edital de Pregão Eletrônico nº 046/CPB/2024 e seus anexos, praticando os valores abaixo discriminados:

LOTE ÚNICO

ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Firewall	2	R$	R$
2	Licença de antivírus	600	R$	R$
3	Implementação e treinamento	1	R$	R$
VALOR TOTAL DA PROPOSTA: R$				

Fica ciente, ainda, que, por ser de seu conhecimento, atende e se submete a todas as cláusulas e condições do Edital que orientará a futura Contratação, bem como às disposições da Lei Federal nº 14.133/2021 e suas alterações posteriores, que integrarão o ajuste correspondente.

Fica ciente, outrossim, que o preço ofertado inclui todos os custos e despesas necessários ao cumprimento integral das obrigações decorrentes da contratação, de modo que nenhuma outra remuneração será devida, afastando qualquer hipótese de responsabilidade solidária pelo pagamento de toda e qualquer despesa, direta ou indiretamente relacionada com o objeto da licitação.

Forma de execução do serviço: conforme edital.
Validade da Proposta: 60 (sessenta) dias.
Condições de Pagamento: Os pagamentos serão efetuados na forma estabelecida no edital.

Início da execução dos serviços: 30 (trinta) dias corridos após assinatura do Contrato.

_____

Responsável (nome/cargo/assinatura)
Nome da Empresa

ANEXO III
DECLARAÇÃO DE QUE NADA DEVE À FAZENDA PÚBLICA DO MUNICÍPIO DE SÃO PAULO

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

AO COMITÊ PARALÍMPICO BRASILEIRO

Eu _____ (nome completo), representante legal da empresa _____ (nome da pessoa jurídica), interessada em participar do Pregão em referência realizado pelo Comitê Paralímpico Brasileiro, declaro sob as penas da lei, que a empresa NÃO é cadastrada como contribuinte no Município de São Paulo e nada deve à Fazenda do Município de São Paulo. Estou ciente de que, se for o caso, o ISS incidente sobre a operação deverá ser retido.

Local e data

_____
Responsável (nome/cargo/assinatura)
Nome da Empresa
Telefone para contato
(Nº do CNPJ da Empresa)

ANEXO IV

DECLARAÇÃO: Constituição Federal – artigo 7º, não há impedimentos em licitar; enquadramento como ME/EPP e Reserva de Cargos

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

A (razão social da proponente), inscrita no CNPJ sob nº ....., por intermédio de seu representante legal o(a) Sr(a). portador(a) da Carteira de Identidade nº..... e do CPF nº ..... DECLARA, sob as penas da Lei:

a) Para fins do disposto no inciso VI, do artigo 68 da Lei Federal nº 14.133/2021, que nos encontramos em situação regular perante o Ministério do Trabalho no que se refere à observância do disposto no inciso XXXIII do artigo 7º da Constituição Federal, não mantendo em nosso quadro de pessoal menores de 18 (dezoito anos) em horário noturno de trabalho ou em serviços perigosos ou insalubres, não possuindo ainda, qualquer trabalho de menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;

b) Que até a presente data inexistem fatos impeditivos para nossa habilitação no presente processo licitatório, assim como que estamos cientes da obrigatoriedade de declarar ocorrências posteriores;

c) Enquadramento da licitante na condição de Microempresa ou Empresa de Pequeno Porte, nos critérios previstos no artigo 3º da Lei Complementar Federal n° 123/2006, bem como sua não inclusão nas vedações previstas no mesmo diploma legal. (excluir caso não se aplique)

D) Que para fins do disposto no inciso IV do art. 63 da Lei Federal n.º 14.133/2021, cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

Local e data

_____

Responsável (nome/cargo/assinatura)
Nome da Empresa
Telefone para contato
(Nº do CNPJ da Empresa)

ANEXO V
DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E ATUAÇÃO CONFORME MARCO LEGAL ANTICORRUPÇÃO

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (nome empresarial), CNPJ nº_____ interessado em participar do Pregão Eletrônico em epígrafe, DECLARO, sob as penas da Lei, especialmente o artigo 299 do Código Penal Brasileiro, que:

a) a proposta apresentada foi elaborada de maneira independente e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

b) o licitante não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

c) o conteúdo da proposta apresentada não foi e nem será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório antes da adjudicação do objeto e;

d) o representante legal do licitante está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

DECLARO, ainda, que a pessoa jurídica que represento conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira e ao CPB, em atendimento à Lei Federal nº 12.846/ 2013 e ao Decreto Estadual nº 60.106/2014, tais como:

I – Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II – Comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;

III – comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV – No tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar licitação ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação ou celebrar contrato administrativo;

f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com o CPB, sem autorização em lei, no ato convocatório da licitação ou nos respectivos instrumentos contratuais; ou

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com o CPB;

V – Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou funcionários, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

Local e data

_____

Responsável (nome/cargo/assinatura)
Nome da Empresa
Telefone para contato
(Nº do CNPJ da Empresa)

ANEXO VI
CADASTRO DE FORNECEDOR

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

DADOS DO FORNECEDOR	
Razão Social:	
CNPJ:	
Endereço:	
Bairro:	
Cidade:	
UF:	
CEP:	
CONTATOS	
Resp. Ass. Contrato:	
CPF:	
RG:	
E-mail:	
Telefone:	
Operacional:	
E-mail:	
Telefone:	
Administrativo:	
E-mail:	
Telefone:	
INFORMAÇÕES ADICIONAIS	
Dados Bancários para Depósito	
Banco:	
Agência:	
Conta Corrente:	

ANEXO VII

QUESTIONÁRIO DE DUE DILIGENCE DE INTEGRIDADE

Por favor, responda as perguntas abaixo de acordo com o melhor do seu conhecimento. Caso seja necessário, informações adicionais podem ser incluídasao final deste formulário.

DADOS SOBRE A SUA EMPRESA OU GRUPO ECONÔMICO ("EMPRESA"): listar e anexar documentos comprobatórios do regular registro do Parceiro.

DADOS DO FORNECEDOR	
Razão Social:	
OUTROS NOMES/NOME FANTASIA:	
CNPJ/MF:	
INSCRIÇÃO MUNICIPAL:	
ENDEREÇO:	
Cidade:	
UF:	
CEP:	
CONTATOS	
TELEFONE:	
SITE/REDE SOCIAL INSTITUCIONAL:	
NÚMERO DE FUNCIONÁRIOS:	
FORMA DE ORGANIZAÇÃO SOCIETÁRIA DA EMPRESA:	

IDENTIFICAR E INFORMAR OS NOMES E ENDEREÇOS DE CONTROLADORA, QUALQUER SUBSIDIÁRIA E/OU COLIGADA, QUALQUER OUTRA EMPRESA OU ENTIDADE NA QUAL DETENHA O CONTROLE ACIONÁRIO E A RESPECTIVA PARTICIPAÇÃO ACIONÁRIA:
INDICAR QUAIS PESSOAS INTEGRAM OU INTEGRARAM, NOS ÚLTIMOS 5 (CINCO) ANOS,A DIRETORIA E O CONSELHO DE ADMINISTRAÇÃO DA EMPRESA:
ACIONISTAS/SÓCIOS (NOME, CPF, NACIONALIDADE E % DE PARTICIPAÇÃO):

a. Objeto social e atividades permitidas pela pessoa jurídica (indicarCNAE na medida do possível):

b. A Empresa é listada na bolsa de valores?

c. Indicar três referências comerciais:

d. Como você ou a Empresa iniciou contato com o Comitê Paralímpico Brasileiro ("CPB") ? Fornecer nome e cargo de quem fez a recomendaçãoou solicitou nosso contato. Se o responsável por lhe apresentar o CPB for algum externo ou terceirizado, favor fornecer o nome da pessoa,CPF/CNPJ e empresa respectiva.

e. Favor indicar o objeto específico desta contratação e a experiência e qualificação da Empresa para prestar tais serviços.

f. Favor indicar o nome, cargo e CPF de todos os funcionários que estarão diretamente responsáveis pela prestação de serviços para oCPB.

II. INTEGRIDADE

a) A Empresa, por meio de seus sócios, diretores ou administradores é, já foi ou possui algum familiar que seja colaborador do CPB? Caso positivo, favor especificar a situação, incluindo o cargo ocupado, período egrau de parentesco.

SIM ( ) | NÃO ( )

b) A Empresa, por meio de seus sócios, diretores ou administradores, éou foi, direta ou indiretamente, controlada por agente público? Caso

positivo, indicar o nome do profissional, o período, cargo ocupado e o órgão em que trabalhou ou trabalha.

SIM ( ) | NÃO ( )

---

c) A Empresa, por meio de seus sócios, diretores ou administradores, possui algum familiar ou pessoa próxima que seja agente público?

Caso afirmativo, indicar o cargo ocupado, período, grau de parentesco e oórgão no qual esta pessoa trabalha.

SIM ( ) | NÃO ( )

---

d) Algum governo ou agência, tanto federal, estadual ou municipal, detém 25% (vinte e cinco por cento) ou mais das ações da Empresa ou, ainda, exerce qualquer espécie de controle ou influência em relação a esta? Caso positivo, favor especificar a situação.

SIM ( ) | NÃO ( )

---

e) A Empresa contrata qualquer espécie de serviço (consultoria ou contabilidade, por exemplo) prestado por Pessoa Politicamente Exposta ou por indivíduo que mantém relacionamento com agentes públicos? Caso positivo, favor especificar a situação, incluindo o cargo ocupado, período, grau de parentesco e/ou relacionamento.

SIM ( ) | NÃO ( )

---

f) A Empresa (ou qualquer empresa do mesmo grupo econômico, ainda que extinta, incorporada ou fundida), por meio de seus sócios, diretores ou administradores, prestadores de serviço, agentes ou outras partes relacionadas foi, nos últimos 10 (dez) anos, parte de algumafiscalização, investigação, processo judicial e/ou administrativo, punição ou avaliação, por parte da Empresa e/ou de qualquer

autoridade competente, por envolvimento em práticas de corrupção, incluindo, mas não se limitando a propina, lavagem de dinheiro, conflito de interesses, improbidade administrativa, fraude fiscal, antitruste e/ou pelo não cumprimento de práticas relacionadas ao programa de integridade? Caso positivo, favor especificar.

SIM ( ) | NÃO ( )

---

g) Há alegações na imprensa de grande circulação ou na imprensa local onde está situada a sede da Empresa, de que algum membro da alta administração ou com cargo de direção, gerência ou supervisão (tal como acionista, sócio, membro do conselho de administração, CEO, diretor, superintendente, gerente, etc.) tenha cometido atos de corrupção e suborno ou lavagem de dinheiro, seja no Brasil ou no exterior? Caso positivo, favor especificar.

SIM ( ) | NÃO ( )

---

h) A Empresa (ou qualquer empresa do mesmo grupo econômico, ainda que extinta, incorporada ou fundida) está ou foi impedida de participar de licitação ou celebrar contratos administrativos ou foi declarada inidônea por qualquer ente federativo ou Poder da Federação? A Empresa consta do Cadastro Nacional de Empresas Punidas – CNEP, do Cadastro Nacional de Empresas Inidôneas ou Suspensas – CEIS oudo Cadastro de Entidades Privadas Sem Fins Lucrativos Impedidas –CEPIM, ou possui algum acordo de leniência vigente? Caso positivo, favor especificar.

SIM ( ) | NÃO ( )

---

i) A Empresa realiza negócios com o governo e/ou participa de licitações? Se sim, qual o percentual da receita da Empresa é originadopor negócios com o governo?

SIM ( ) | NÃO ( )

---

j) A Empresa realiza doações e patrocínios? Se sim, explicar os procedimentos para concessão de doações e patrocínios, incluindo o fluxode aprovação e as diligências realizadas.

SIM ( ) | NÃO ( )

k) A Empresa manterá interações com agentes públicos ou Pessoas Politicamente Expostas em nome do CPB em virtude da prestação de serviços? Caso positivo, favor especificar.

SIM ( ) | NÃO ( )

l) A Empresa, por meio de seus sócios, diretores ou administradores, possui alguma outra atividade ou algum outro relacionamento que possa potencialmente caracterizar um conflito de interesses que nãofoi abrangido pelas perguntas acima? Caso positivo, favor especificar.

SIM ( ) | NÃO ( )

III. PREVENÇÃO À LAVAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA:

a) A empresa possui Política de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa? Em caso positivo, indicar o diretor responsável pelo Programa.

SIM ( ) | NÃO ( )

b) A empresa possui procedimento para conhecer seus parceiros, funcionários e clientes (Know Your Customer, Know Your Employee, Know Your Supplier/Partner)?

SIM ( ) | NÃO ( )

c) A empresa tem programa de prática de conscientização (treinamentoe comunicação) em Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP), incluindo terceiros - parceiros e fornecedores?

SIM ( ) | NÃO ( )

IV. ADMINISTRADORES E SÓCIOS DA EMPRESA:

a) Caso aplicável, liste todas as pessoas físicas ou jurídicas, membros do Conselho de Administração e Diretores Estatutários da Empresa que detenham participação acionária significativa na Empresa, 5% (cincopor cento) ou mais ("Proprietários"), incluindo cargo e CPF/CNPJ.

b) Caso aplicável, liste todos os Proprietários da Empresa que detenham participação acionária significativa, 5% (cinco por cento) ou mais, e/ouque possuam cargos em outra empresa. Indique, ainda, o nome das respectivas empresas.

c) Caso aplicável, liste todos os Proprietários que são, foram ou possuam relacionamento com agente público e/ou Pessoas Politicamente Expostas.

V. SUBCONTRATAÇÃO E REMUNERAÇÃO:

a) Qual a forma de pagamento a ser utilizada no âmbito da contração? Haverá alguma condição especial, como taxa de sucesso, valor adiantado ou reembolso de despesas? Caso positivo, favor especificar.

b) A Empresa fará qualquer tipo de pagamento em nome do CPB? Caso positivo, favor especificar.

c) A prestação de serviços será realizada apenas pela Empresa ou haverá subcontração e/ou participação de representantes externos? Caso positivo, favor especificar e indicar o nome dos respectivos representantes externos e empresas, bem como CNPJ ou CPF, endereço e as atividades a serem realizadas por estes.

d) Haverá interação dos subcontratados e/ou representantes externos com agentes públicos e entidades governamentais, incluindo empresas estatais? Caso positivo, favor especificar.

e) A Empresa exige que seus subcontratados e representantes externos sigam o disposto em seu Código de Ética, bem como cumpram a legislação vigente, especialmente no que tange às leis anticorrupção? Favor detalhar.

VI. RESPONSÁVEL PELO PREENCHIMENTO DO FORMULÁRIO:

Declaro e atesto para os devidos fins que as informações fornecidas anteriormente, bem como os documentos disponibilizados são verdadeiros e não ocultaram quaisquer dados. Se, em algum momento, as informações ou documentos apresentados neste questionário não representarem mais a realidade, concordo em comunicar imediatamente Comitê Paralímpico Brasileiro – CPB - e fornecer um relatório complementar detalhando referida mudança.

NOME CPF:

CARGO OU FUNÇÃO:

Telefone para contato

ANEXO VIII
MINUTA DE CONTRATO

PROCESSO Nº 0696/2024

CÓDIGO DO ÓRGÃO XXXXXXXX

MODALIDADE: PREGÃO ELETRÔNICO Nº 046/CPB/2024

OBJETO: Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital

Pelo presente instrumento, de um lado, o **COMITÊ PARALÍMPICO BRASILEIRO**, inscrito no CNPJ sob o n.º 00.700.114/0001-44, com sede na Rodovia dos imigrantes, km 11,5 - CEP: 04329-000 – Vila Guarani – São Paulo/SP, representado por seu Presidente, o Sr. **XXXXX** ,portador da carteira de identidade RG n.º **XXXXX**, inscrito no CPF/MF sob o nº **XXXXX**, doravante denominado simplesmente **CONTRATANTE**, e de outro, **XXXXX**, inscrita no CNPJ sob o n.º **XXXXX**, com sede à **XXXXX**, representada por **XXXXXXXXXXXXXX**, portador da carteira de identidade RG nº **XXXXX**, e inscrito no CPF/MF sob o nº **XXXXX**, doravante designada simplesmente **CONTRATADA**, em conformidade com o Processo **nº 0696/2024** e com os termos do REGULAMENTO DE AQUISIÇÕES E CONTRATOS aprovado pela RESOLUÇÃO CPB Nº 01, de abril de 2023, celebram o presente contrato com base nas cláusulas e condições que seguem.

1. CLAUSULA PRIMEIRA DO OBJETO

1.1. O presente contrato tem por objeto a **Prestação de serviço de solução de firewall e antivírus, conforme especificações constantes do Termo de Referência Anexo I do Edital** do Pregão Eletrônico nº **046/CPB/2024**, instrumento do qual deriva este presente contrato.

1.2. O fornecimento do(s) item(s) deverá(ao) seguir os procedimentos e especificações constantes do Anexo I - Termo de Referência.

1.3. Este instrumento guarda inteira conformidade com os termos do **Pregão Eletrônico n° 046/CPB/2024**, do qual faz parte integrante e complementar, vinculando-se ainda à proposta da CONTRATADA e demais anexos do processo, independente de transcrição.

2. CLAUSULA SEGUNDA DO VALOR CONTRATUAL

2.1. Pelo fornecimento do objeto deste contrato, o CONTRATANTE pagará à CONTRATADA o valor total de R$ XXXX (xxxx); conforme quadro descritivo no item 2.2.

2.1.1. Este (s) preço (s) inclui todos os custos, impostos, taxas, benefícios e constituirá, a qualquer título, a única e completa remuneração pelo adequado

e perfeito cumprimento do objeto das obrigações do presente contrato, de modo que nenhuma outra remuneração será devida.

2.2. Quadro Descritivo:

LOTE ÚNICO

ITEM	DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Firewall	2	R$	R$
2	Licença de antivírus	600	R$	R$
3	Implementação e treinamento	1	R$	R$
VALOR TOTAL DA PROPOSTA: R$				

3. CLÁUSULA TERCEIRA – DOS PREÇOS E DO REAJUSTE

3.1. Os preços oferecidos remunerarão todas as despesas com a execução dos serviços citados, e devem compreender todos os custos de mão de obra, transportes, encargos sociais, previdenciários, fiscais, trabalhistas e demais despesas necessárias à correta execução do objeto.

3.2. O preço contratual poderá ser reajustado de acordo com a variação do IPCA, após 01 (um) ano da data da assinatura do contrato, ficando vedado novo reajuste pelo prazo de um ano.

3.3. Fica ressalvada a possibilidade de alteração das condições contratuais, em face da superveniência de normas federais disciplinando a matéria.

4. CLÁUSULA QUARTA – DA VIGÊNCIA CONTRATUAL

4.1. O presente contrato vigorará por 12 (doze) meses, contados a partir da data de sua assinatura, podendo a contratação ser prorrogada, mediante a celebração de termo aditivo, limitado o somatório do tempo das prorrogações ao máximo de 120 (cento e vinte) meses, contados da data da celebração do contrato.

5. DA CLÁUSULA QUINTA - DO PAGAMENTO

5.1. O pagamento será efetuado em até 30 (trinta) dias corridos a contar do atesto da nota fiscal, mediante a apresentação do(s) relatório(s), da nota fiscal de fornecimento executados, atestada pelo departamento demandante, responsável pelo recebimento dos produtos, materiais e/ou equipamentos.

5.2. Após devidamente atestada pelo responsável pelo recebimento, a Nota Fiscal será encaminhada para pagamento que ocorrerá em até 30 (trinta) dias corridos, devendo

ser efetuada a retenção na fonte dos tributos e contribuições determinadas pelos órgãos fiscais e fazendários em conformidade com a legislação vigente, quando for o caso.

5.2.1. A discriminação dos valores e dos equipamentos, materiais e/ou produtos deverão ser reproduzidos na nota fiscal apresentada para efeito de pagamento a qual deverá ser encaminhada para o e-mail nf@cpb.org.br.

5.2.2. O não envio da nota fiscal para o e-mail nf@cpb.org.br poderá ocasionar atrasos nos tramites de liquidação.

5.3. O CPB poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela empresa contratada, nos termos do Edital e seus anexos.

5.4. Nenhum pagamento será efetuado à empresa contratada na pendência de: manutenção das condições de habilitação, comprovação de fornecimento e cumprimento de obrigações assumidas.

5.5. O CNPJ da documentação fiscal deverá ser o mesmo da proposta de preço apresentada no respectivo procedimento de aquisição, sob pena de rescisão contratual.

5.6. A CONTRATADA deverá emitir a Nota Fiscal, acompanhada da documentação a seguir:

5.6.1. Regularidade Fiscal

5.6.1.1. Comprovante de Inscrição e de Situação Cadastral de Pessoa Jurídica no site do Ministério da Fazenda;

5.6.1.2. Certidão de regularidade perante o FGTS;

5.6.1.3. Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União;

5.6.1.4. Certidão Negativa de Débitos Trabalhistas;

5.6.1.5. Certidão de Regularidade para com a Fazenda Municipal da sede ou domicílio da licitante.

5.6.2. Regularidade Trabalhista

5.6.2.1. Enviar quando solicitado a documentação necessária que comprove o cumprimento das obrigações sociais, trabalhistas, tributárias e fiscais.

5.7. No caso de constatação de erros ou irregularidades no documento fiscal comprobatório ou ausência da documentação constante do item 5.6, o prazo de pagamento será interrompido e reiniciará somente após a apresentação de nova documentação, devidamente corrigida.

5.8. Nenhum pagamento será efetuado enquanto houver pendência de liquidação de obrigação financeira ou contratual em virtude de penalidade aplicada.

5.9. No caso de constatação de erros ou irregularidades no documento fiscal comprobatório ou ausência da documentação que comprove a regularidade fiscal e trabalhista da CONTRATADA, o prazo de pagamento será interrompido e reiniciará somente após a apresentação de nova documentação, devidamente corrigida.

5.10. Nenhum pagamento será efetuado enquanto houver pendência de liquidação de obrigação financeira ou contratual em virtude de penalidade aplicada.

5.11. Previamente ao pagamento, a CONTRATANTE poderá realizar consulta aos órgãos competentes para ratificar a situação de regularidade da CONTRATADA relativamente às condições de habilitação exigidas.

6. DA CLÁUSULA SEXTA - DAS OBRIGAÇÕES

6.1. Além das obrigações constantes descritas no Termo de Referência, Anexo I do Edital de **Pregão Eletrônico nº 046/CPB/2024**, cabe à CONTRATADA:

6.1.1. Garantir que os serviços sejam executados por equipe técnica profissional devidamente qualificada e com experiência no segmento do objeto deste contrato.

6.1.2. Disponibilizar toda a mão-de-obra, equipamentos, acessórios e materiais necessários à execução dos serviços, que deverão fazer parte dos custos do contrato.

6.1.3. Prestar ao Comitê Paralímpico Brasileiro, sempre que necessário, esclarecimentos, bem como apresentação de relatórios de execução sobre os serviços prestados, fornecendo toda e qualquer orientação necessária para a perfeita utilização.

6.1.4. Manter-se durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no momento da licitação.

6.1.5. Responsabilizar-se única e exclusivamente, pelo pagamento de todos os encargos e demais despesas decorrentes da prestação de serviço, tais como

impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, por mais especiais que sejam e mesmo que não expressas na presente contratação.

6.1.6. Responsabilizar-se integralmente por todas as despesas decorrentes de:

a) Transporte, montagem, desmontagem, instalação, programação, operação, acompanhamento, manutenção, guarda e vigilância dos materiais, documentos e equipamentos.

b) Mão-de-obra, alimentação, transporte, hospedagem, assistência médica e de pronto-socorro que forem devidas a sua equipe.

c) E outras que porventura venham a incidir na referida execução.

6.1.7. Responsabilizar-se por seguro contra incêndio, roubo, acidentes que porventura possam ocorrer com equipe, documentos equipamentos e terceiros, isentando a CONTRATANTE de qualquer indenização ou ressarcimento.

6.1.8. Fornecer, toda a supervisão, direção técnica e administrativa e mão de obra qualificada necessária à execução dos serviços contratados, bem como também, todos os materiais e equipamentos ofertados em sua proposta comercial e documentos pertinentes a prestação dos serviços.

6.1.9. Facilitar, por todos os meios ao seu alcance, a ampla ação da fiscalização da CONTRATANTE, provendo o fácil acesso aos serviços em execução e atendendo prontamente as observações, exigências, recomendações técnicas e administrativas por ela apresentadas.

6.1.10. Providenciar a retirada imediata de qualquer empregado seu, cuja permanência seja considerada inconveniente para a adequada prestação dos serviços.

6.1.11. Indicar o preposto que o representará a prestação dos referidos serviços, para receber as instruções, bem como propiciar à equipe de fiscalização da CONTRATANTE, toda a assistência e facilidade necessárias ao bom e adequado cumprimento e desempenho de suas tarefas.

6.1.12. Responsabilizar-se pelos danos causados à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do Contrato. Não exclui ou reduz essa responsabilidade a fiscalização efetuada pela gestão da CONTRATANTE.

6.1.13. Responder civil e criminalmente pela atuação de seus profissionais.

6.1.14. Manter todos os equipamentos, locais de armazenamento e utensílios necessários à execução dos serviços, em perfeitas condições de uso, devendo os danificados serem substituídos.

6.1.15. Aceitar nas mesmas condições contratuais acréscimos até o limite de 50% (cinquenta por cento) do valor inicial atualizado do contrato, permitida a supressão além do limite de 25% (vinte e cinco por cento), desde que mediante acordo entre as partes;

6.1.16. Cumprir, às suas próprias expensas, todas as cláusulas contratuais e deste Termo que definam suas obrigações;

6.1.17. Executar e cumprir os serviços e prazos mencionados no Termo de Referência;

6.1.18. Não reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado conhecimento em razão da prestação de serviços objeto do presente, sem o consentimento por escrito do CPB;

6.1.19. Esclarecer, toda e qualquer dúvida que lhe seja apresentada pela CONTRATANTE, no tocante a execução dos serviços, objeto do Contrato.

6.1.20. Responsabilizar-se integralmente pelos serviços contratados, cumprindo as disposições legais e regulamentares federais, estaduais e municipais que interfiram na execução dos serviços, inclusive de segurança e medicina do trabalho e de segurança pública, bem como, as normas da Associação Brasileira de Normas Técnicas (ABNT), sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa;

6.1.21. Caso a contratante venha a ser demandada por terceiros que se julguem prejudicados, bem como venha experimentar prejuízo patrimonial em decorrência dos serviços prestados pela contratada, esta deverá se responsabilizar pelos pagamentos, indenizações e reembolsos que se façam necessários, inclusive mediante retenção de valores de pagamento se houver contratos ainda vigentes, ou ainda por medidas judiciais cabíveis se a contratada já não mais prestar serviços à contratante.

6.1.22. Efetuando-se qualquer retenção nos pagamentos da contratada, nos termos do item anterior, para fazer frente à responsabilização civil, e havendo condenação em valor inferior, a contratante devolverá à contratada o saldo entre o valor retido, sem adicionais de qualquer natureza, e o total do valor da indenização, acrescido das respectivas custas com o processo.

6.1.23. É vedada a veiculação de publicidade acerca do objeto.

6.1.24. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e o CPB, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

6.1.25. Dar ciência imediata e por escrito à CONTRATANTE de qualquer irregularidade relacionada com os serviços que possa comprometer sua execução e o bom andamento das atividades.

6.1.26. Fazer seguro de seus empregados contra riscos de acidentes de trabalho, responsabilizando-se, também, pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do Contrato, conforme exigência legal.

6.1.27. Fornecer, com no máximo dois dias de antecedência da data da execução dos serviços, uma relação dos profissionais (recursos humanos) contendo nome completo, RG e CPF, modelo e placa dos veículos utilizados na atividade, para a liberação deles na portaria, por motivos de segurança.

6.2. Além das obrigações constantes no Edital de Pregão Eletrônico nº 046/CPB/2024, cabe à CONTRATANTE:

6.2.1. Designar Fiscal responsável pelo acompanhamento dos Serviços/Contrato.

6.2.2. Responsabilizar-se pelo acompanhamento e fiscalização da execução da presente contratação, através do Fiscal da "CONTRATANTE", que deverá anotar, em registro próprio, todas as ocorrências verificadas.

6.2.3. Comunicar, imediatamente, por escrito, à "CONTRATADA" qualquer irregularidade observada no decorrer da execução dos serviços.

6.2.4. Esclarecer, prontamente, as dúvidas que lhe sejam apresentadas.

6.2.5. Acompanhar e fiscalizar, os trabalhos a serem desenvolvidos pela Contratada, visando o atendimento das normas, especificações e instruções estabelecidas, devendo intervir quando necessário, a fim de assegurar sua regularidade e o fiel cumprimento.

6.2.6. Expedir, por escrito, as determinações e comunicações dirigidas à Contratada.

6.2.7. Poderá, a seu critério e a qualquer tempo, realizar vistoria dos equipamentos utilizados na execução dos serviços e verificar o cumprimento de normas preestabelecidas no contrato ou em decorrência de norma específica que rege a prestação de serviços objeto do presente.

6.2.8. Rejeitar, no todo ou em parte, o fornecimento e/ou a prestação de serviço que estiver em desacordo com este Termo de Referência, podendo até aplicar penalidades ou rompimento do contrato.

6.2.9. Aplicar, quando for o caso, as penalidades previstas neste ajuste de acordo com o edital e as leis que regem a matéria.

6.2.10. Encaminhar ao setor responsável, a liberação de pagamento da Nota Fiscal da prestação dos serviços aprovados.

6.2.11. Proporcionar ao pessoal técnico da CONTRATADA todas as facilidades operacionais e condições necessárias ao pleno desenvolvimento das atividades atinentes à execução dos serviços e permitir acesso do pessoal da "CONTRATADA" às instalações, respeitando-se as normas da "CONTRATANTE", no que tange a horários e segurança.

6.2.12. Disponibilizar para a CONTRATADA, a tempo e modo, todas as informações, documentos ou quaisquer outras solicitações necessárias.

6.2.13. Proceder às retenções de tributos ou outros encargos fiscais previstos em Lei, e que por força desta, se lhe impõe tal atribuição, devendo providenciar o repasse ao órgão ou entidade credora na forma e condições previstas na legislação de regência.

6.2.14. Atestar os serviços da CONTRATADA, mediante relatório, de forma a relatar ocorrências da prestação dos serviços.

6.2.15. Efetuar o pagamento ajustado dos serviços prestados pela "CONTRATADA", após atestar a nota fiscal.

6.2.16. Analisar a solicitação de adequações e reparos, caso seja emitida pelos colaboradores da Contratada, que são indispensáveis ao perfeito funcionamento das atividades desenvolvidas.

6.2.17. Executar qualquer serviço que a CONTRATADA venha a julgar necessário à segurança e ao bom funcionamento do(s) equipamento(s) ou, se for o caso, autorizar sua execução, respondendo junto à fiscalização competente pelo não cumprimento das determinações legais.

6.2.18. Encaminhar a liberação de pagamento da Nota Fiscal da prestação do serviço aplicando-se os devidos fatores de desconto, conforme relatório de avaliação da qualidade dos serviços prestados.

6.2.19. Examinar a qualquer tempo toda documentação da Contratada, para comprovar suas condições de habilitação.

7. **CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO**

7.1. A fiscalização do contrato será exercida pelo XXXXXXXXXXX, responsável pelo Departamento de Tecnologia da Informação do CPB, ou, em caso de ausência, ao funcionário que o esteja substituindo, a quem caberá dirimir as dúvidas porventura surgidas no curso da prestação dos serviços, bem como adotar as medidas que se fizerem necessárias para o seu bom e fiel cumprimento.

7.2. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades e não implica em co-responsabilidade do CONTRATANTE.

7.3. O CONTRATANTE se reserva o direito de rejeitar no todo ou em parte os serviços prestados, se considerados em desacordo com o contrato ou proposta da CONTRATADA.

8. CLAUSULA OITAVA – DAS ALTERAÇÕES

8.1. O presente contrato poderá ser alterado, no interesse do CONTRATANTE, por acordo entre as partes, mediante termo aditivo, e com as devidas justificativas, nos seguintes casos:

I. Unilateralmente, pelo CONTRATANTE:

a) Quando houver modificação do projeto ou das especificações, para melhor adequação técnica a seus objetivos;

b) Quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, no limite permitido.

II. Por acordo das partes:

a) Quando conveniente a substituição da garantia de execução;

b) Quando necessária a modificação do regime de execução do recebimento, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

c) Quando necessária à modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, sem a correspondente comprovação do fornecimento de bens;

d) Para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de

fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.

9. **CLÁUSULA NONA - DAS SANÇÕES ADMINISTRATIVAS**

9.1. Além das sanções previstas no capítulo I, do Título IV da Lei Federal nº 14.133/2021, e demais normas pertinentes, também poderão ser aplicadas à CONTRATADA as seguintes penalidades pela inadimplência das obrigações contratuais, sendo-lhe assegurados o contraditório e a ampla defesa.

9.1.1. Multa de 30% (trinta por cento) pela recusa em Assinar o Contrato, dentro do prazo estabelecido ou fazê-lo com atraso, sem a devida justificativa aceita pelo CPB, a qual incidirá sobre o valor do ajuste.

9.1.2. Incidirá na mesma penalidade a não apresentação dos documentos necessários a celebração do ajuste.

9.1.3. Advertência, para os casos de infração de menor potencial e desde que não haja prejuízo para o CONTRATANTE.

9.1.4. Multa de 10% (dez por cento) sobre o valor do Contrato ou Ordem de Serviço no atraso no início ou durante a prestação de serviços, ou no caso de execução em desacordo com o previsto em termo;

9.1.5. Caso a execução seja feita de forma parcial, o percentual da multa por atraso incidirá sobre o valor total do(s) serviços prestados(s) em atraso.

9.1.6. Multa de 15% (quinze por cento) sobre o valor total do Contrato ou da ordem de Serviço, pela inexecução parcial dos serviços;

9.1.6.1. Caso a execução do serviço seja feita de forma parcial, o percentual da multa por inexecução parcial, incidirá sobre o valor total do(s) serviços(s) não prestado(s).

9.1.7. Multa de 30% (trinta por cento) sobre o valor total do Contrato ou da Ordem de serviços pela inexecução total do contrato, respectivamente.

9.1.8. Multa de 2% (dois por cento) a 10% (dez porcento), a depender da gravidade da falta, sobre o valor do Contrato ou da Ordem Serviço, por descumprimento de qualquer das obrigações decorrentes do ajuste, não previstas nas demais penalidades.

9.1.9. O inadimplemento total ou parcial das obrigações assumidas dará ao CPB o direito de rescindir unilateralmente o Contrato, sem prejuízo das outras penalidades previstas.

9.1.10. As penalidades poderão ser aplicadas cumulativamente, conforme dispõe §7°, do art. 156, da Lei Federal nº 14.133/2021.

9.1.11. O valor da multa aplicada poderá ser compensado com crédito em favor da Contratante.

9.1.12. Sendo a multa de valor superior aos pagamentos eventualmente devidos pelo CPB, a Contratada responderá pela sua diferença, devendo realizar o pagamento em favor do CPB no prazo de 5 (cinco) dias úteis a contar da notificação de aplicação de penalidade, sob pena ser cobrada judicialmente.

9.1.13. Em caso de inadimplemento da multa imposta o valor será corrigido pelo índice IPCA e sofrerá incidência de juros de mora de 1% ao mês.

10. CLÁUSULA DÉCIMA – DA RESCISÃO CONTRATUAL

10.1. Constituem motivo para rescisão do contrato:

I. Não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

II. Desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;

III. Alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;

IV. Decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;

V. Caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;

VI. Não cumprimento das obrigações relativas à reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

10.2. A rescisão do contrato poderá ser:

I. Determinada por ato unilateral e escrito do CPB, exceto no caso de descumprimento decorrente de sua própria conduta;

II. Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse do CPB;

III. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

11. DA CLÁUSULA DÉCIMA PRIMEIRA – DO TRATAMENTO DOS DADOS PESSOAIS

11.1. As partes declaram estar cientes das regras e princípios relacionados com a proteção de dados pessoais previstos na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados ("LGPD") - e nas demais determinações de órgãos reguladores e fiscalizadores sobre a matéria, e concordam com a sua observância para realização de qualquer atividade de tratamento de dados pessoais, necessárias para a execução do objeto deste CONTRATO.

11.2. Os dados pessoais coletados incluem, mas não se limitam, as informações de qualificação dos representantes legais, nome e documento das testemunhas e nomes e contato de colaboradores e de prestadores de serviço. A finalidade da sua coleta é para a execução do objeto deste CONTRATO, conforme disposto no Art. 7º, inciso V, da LGPD.

11.3. Os dados pessoais de colaboradores e prestadores de serviço, que porventura forem coletados na execução deste CONTRATO, também poderão ser necessários para atender os interesses legítimos da CONTRATANTE, nos termos do art. 7º, inciso IX, da LGPD.

11.4. As partes se obrigam a proteger os dados pessoais a que venham a ter acesso em virtude ou em consequência da execução deste CONTRATO, por meio da adoção de medidas técnicas, físicas e organizacionais de segurança da informação, bem como se obrigam ao dever de confidencialidade, integridade e sigilo, devendo assegurar que os seus colaboradores, consultores e prestadores de serviços que, no exercício das suas funções tenham acesso ou conhecimento das informações e dados pessoais tratados, estejam, igualmente e por contrato, obrigados ao sigilo profissional. O descumprimento da presente cláusula ensejará a imediata rescisão deste CONTRATO, sem prejuízo de eventual responsabilidade civil ou criminal.

12. DA CLÁUSULA DÉCIMA SEGUNDA - DAS DISPOSIÇÕES FINAIS

12.1. As partes declaram conhecer as normas de responsabilização, combate e prevenção à corrupção previstas na legislação brasileira, em especial os dispositivos do Código Penal Brasileiro, da Lei de Improbidade Administrativa (Lei nº 8.429/1992), da Lei nº 12.846/2013 (Lei Anticorrupção) e do Decreto 11.129/2022, bem como do Código de

Conduta Ética e das Políticas de Integridade do CPB , e se comprometem a cumpri-las fielmente, por si e por seus funcionários e colaboradores, bem como exigir o seu cumprimento pelos terceiros por ela contratados. Adicionalmente, as PARTES desde já se obrigam a não dar, oferecer ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto do contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos, colaboradores e quaisquer terceiros relacionados ajam da mesma forma.

12.2. Os signatários deste CONTRATO declaram, sob as penas da Lei, que são representantes legais das Partes aqui estabelecidas, devidamente constituídos dos respectivos Estatutos/Contratos Sociais ou com procuração contendo plenos poderes para assumir as obrigações ora contraídas.

12.3. As partes aceitam integralmente que as assinaturas do CONTRATO possam ser realizadas através de assinatura eletrônica, sendo o presente CONTRATO irrevogavelmente considerado por todos que o assinam, com prova documental e título executivo extrajudicial, para todos os fins e efeitos.

12.4. Fica ressalvada a possibilidade de alteração das condições contratuais em face da superveniência de normas federais e/ou municipais que as autorizem.

12.5. A CONTRATADA, fica ciente de que a assinatura deste termo indica que tem pleno conhecimento dos elementos nele constantes, bem como de todas as condições gerais e peculiares de seu objeto, não podendo invocar qualquer desconhecimento quanto aos mesmos, como elemento impeditivo do perfeito cumprimento de seu objeto.

12.6. Aplicam-se a este contrato todas as disposições do instrumento convocatório, mediante edital de PREGÃO ELETRÔNICO Nº 046/CPB/2024, que é parte integrante deste Instrumento, independentemente de transcrição.

12.7. Fica a contratada ciente de que a simples assinatura deste implica aceitação de todas as suas cláusulas e condições.

12.8. Os casos omissos serão resolvidos com base na legislação aplicável aos contratos administrativos.

12.9. A CONTRATADA deverá comunicar ao CONTRATANTE toda e qualquer alteração nos dados cadastrais, para atualização, sendo sua obrigação manter, durante a vigência do presente, compatibilidade com as obrigações assumidas, todas as condições de

habilitação e qualificação exigidas no Edital de **PREGÃO ELETRÔNICO Nº 046/CPB/2024.**

13. DA CLÁUSULA DÉCIMA TERCEIRA - DO FORO

13.1. Fica eleito o Foro do Município de São Paulo, com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer questões oriundas deste contrato.

13.2. E, assim, por estarem justas e acordadas as partes firmam o presente instrumento, com a ciência das testemunhas abaixo assinadas, para que produza os seus efeitos jurídicos e legais.

São Paulo, XX de XXXXXX de 2024.

CONTRATANTE	CONTRATADA
TESTEMUNHAS:	
1 -	2 -