PREGÃO ELETRÔNICO

90059/2025

CONTRATANTE (UASG)

Fundação Centro de Atendimento Socioeducativo ao Adolescente – Fundação CASA-SP

990202

OBJETO

Contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes

VALOR TOTAL DA CONTRATAÇÃO

Sigiloso

DATA DA SESSÃO PÚBLICA

Dia **09/06/2025** às **09h30 (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

menor preço global

MODO DE DISPUTA:

aberto

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM

PREÂMBULO

PREGÃO ELETRÔNICO Nº 90059/2059

Processo Administrativo SEI n° 161.00039823/2025-01

Código Único nº 20250393291

Torna-se público que a Fundação Centro de Atendimento Socioeducativo ao Adolescente – **Fundação CASA-SP**, por meio da Divisão de Suprimentos, sediada na **Rua Florêncio de Abreu, n.º 848 - 7º andar - Luz - São Paulo - SP - CEP 01030-001**, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto estadual nº 67.608, de 27 de março de 2023, da Portaria Normativa nº 444/2024 e demais normas da legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital e em seus Anexos.

1. DO OBJETO

1.1. O objeto da presente licitação é a contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes, conforme condições, quantidades e exigências estabelecidas neste Edital e seus Anexos.

1.2. A licitação será realizada em único item.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.1.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.2. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no subitem anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.3. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

2.4. Nos limites previstos no art. 4º da Lei nº 14.133, de 2021, e na Lei Complementar nº 123, de 2006, serão observadas, caso aplicáveis, as regras de tratamento favorecido para as microempresas e empresas de pequeno porte, para as cooperativas que atendam ao disposto no art. 34 da Lei n° 11.488, de 2007, e no art. 16 da Lei nº 14.133, de 2021 e para o microempreendedor individual – MEI.

2.5. Em relação às regras aplicáveis à presente licitação concernentes a tratamento favorecido para as microempresas, empresas de pequeno porte e equiparadas, observa-se que:

2.5.1. A participação é ampla, sendo aplicáveis as regras de tratamento favorecido constantes dos arts. 42 a 45 da Lei Complementar nº 123, de 2006, observado o disposto no § 2º do art. 4º da Lei nº 14.133, de 2021.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) Anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários, observado o disposto nos §§ 2º e 4º do art. 14 da Lei nº 14.133, de 2021;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público 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. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. 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;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. aquele que não tenha representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente.

2.7. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade licitante ou contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7.1. A vedação de participação de agente público do órgão ou entidade licitante ou contratante de que trata o subitem anterior estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

2.8. O impedimento decorrente de imposição de sanção de que trata o subitem 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.9. No que concerne aos subitens 2.6.2 e 2.6.3, equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. Será permitida a participação de sociedades cooperativas nesta licitação, nos termos do art. 16 da Lei nº 14.133, de 2021.

2.11. Será admitida a participação de pessoas jurídicas em consórcio, nos termos do art. 15 da Lei nº 14.133, de 2021.

2.11.1. Será vedada a participação de empresa consorciada, na mesma licitação, de mais de um consórcio ou de forma isolada, nos termos do art. 15, inc. IV, da Lei nº 14.133, de 2021.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.3.1. está ciente e concorda com as condições contidas no Edital e seus Anexos, bem como que a proposta apresentada compreenderá a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.3.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição Federal;

3.3.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.3.4. 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.

3.4. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.5. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa que atenda ao disposto no art. 34 da Lei nº 11.488, de 2007 deverá declarar, ainda, em campo próprio do sistema eletrônico, 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 arts. 42 a 49.

3.5.1. Não se aplica o tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, na hipótese em que item objeto desta licitação tenha valor estimado superior ao limite estabelecido nos §§ 1º e 3º do art. 4º da Lei nº 14.133, de 2021, conforme seja especificado, quando houver, no item 2.

3.5.2. Não têm direito ao tratamento favorecido estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, as microempresas, as empresas de pequeno porte e as cooperativas que, no ano-calendário de realização da licitação, tenham celebrado contratos

com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, nos termos do § 2º do art. 4º da Lei nº 14.133, de 2021.

3.5.3. Na hipótese de se verificar a exceção especificada no subitem 3.5.1 ou no subitem 3.5.2, o licitante deverá assinalar o campo “não”, por não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006.

3.5.4. No item exclusivo para participação de microempresas, empresas de pequeno porte e equiparadas, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item.

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

3.6. A falsidade da declaração de que trata os subitens 3.3 a 3.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.7. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

3.8. Não haverá ordem de classificação na etapa de apresentação da proposta pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.9. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.10. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.10.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.10.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.11. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado valor superior a lance já registrado pelo fornecedor no sistema.

3.12. O valor final mínimo parametrizado na forma do subitem 3.10 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos campos relacionados ao valor unitário e total do item.

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Independentemente do percentual de tributo inserido na planilha, quando houver determinação legal de retenção de tributo, no pagamento serão retidos na fonte os percentuais que sejam estabelecidos na legislação vigente.

4.6. As microempresas e empresas de pequeno porte impedidas de optar pelo Simples Nacional, ante as vedações previstas na Lei Complementar nº 123, de 2006, não poderão aplicar os benefícios decorrentes desse regime tributário diferenciado em sua proposta, devendo elaborá-la de acordo com as normas aplicáveis às demais pessoas jurídicas.

4.6.1. Quando for o caso, e se vier a ser contratado, o licitante na situação descrita no subitem anterior deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que ocorrida a situação de vedação, nos termos do art. 30, caput, inc. II, e § 1º, inc. II, da Lei Complementar nº 123, de 2006, apresentando à Administração a comprovação da exclusão ou o seu respectivo protocolo.

4.6.2. Se o Contratado não realizar espontaneamente o requerimento de que trata o subitem anterior, caberá ao ente público contratante comunicar o fato ao órgão fazendário competente, solicitando que o Contratado seja excluído de ofício do Simples Nacional, nos termos do art. 29, inc. I, da Lei Complementar nº 123, de 2006.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe a documentação que integra este Edital, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de utilizar os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

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

4.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas.

4.10. O descumprimento das regras supramencionadas por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas competente e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição Federal, e do art. 33, inc. X, da Constituição do Estado de São Paulo; ou condenação dos agentes públicos responsáveis e do contratado ao pagamento de indenização pelos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor total global da contratação.

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de:

Item Serviço	**Intervalo mínimo de valores**
1	3.000,00

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa "**aberto**", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

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

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

5.10.3. Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.10.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

5.10.5. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

5.11. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

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

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

5.14. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.15. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.16. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.17. Uma vez que a presente licitação não é de participação exclusiva de microempresas e empresas de pequeno porte, não se aplica o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006.

5.18. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa “aberto e fechado”.

5.19. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei nº 14.133, de 2021;

5.19.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.20. Persistindo o empate, será assegurada preferência, nos termos do § 1º do art. 60 da Lei nº 14.133, de 2021, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.20.1. empresas estabelecidas no território do Estado de São Paulo;

5.20.2. empresas brasileiras;

5.20.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.20.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.21. Encerrada a etapa de envio de lances da sessão pública, na hipótese de a proposta do primeiro colocado permanecer acima do preço máximo, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.21.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.21.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.21.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.21.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.21.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante antes de findo o prazo, ou de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio da documentação exigida.

5.22. Após a negociação do preço, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133, de 2021, legislação correlata e no subitem 2.6 deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/sancoes/consulta);

6.1.4. Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade – CNCIAI, do Conselho Nacional de Justiça (http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php);

6.1.5. Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções (http://www.esancoes.sp.gov.br);

6.1.6.Cadastro Estadual de Empresas Punidas – CEEP (http://www.servicos.controladoriageral.sp.gov.br/PesquisaCEEP.aspx); e

6.1.7. Relação de apenados publicada pelo Tribunal de Contas do Estado de São Paulo (https://www.tce.sp.gov.br/apenados).

6.2. A consulta ao cadastro CNCIAI será realizada em nome da pessoa jurídica licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, *caput*, c/c Decreto estadual nº 67.608, de 2023).

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 1º, c/c Decreto estadual nº 67.608, de 2023).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 29, § 2º, c/c Decreto estadual nº 67.608, de 2023).

6.3.3. Constatada a existência de sanção, o licitante será considerado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, prosseguirá a análise da fase de julgamento da proposta classificada em primeiro lugar.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido a microempresas e empresas de pequeno porte, o pregoeiro verificará se faz jus ao benefício, em conformidade com os subitens 2.5 e 3.5 deste Edital.

6.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus Anexos.

6.6.1. Se a proposta vencedora for desclassificada, o pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

6.6.2. Encerrada a fase de julgamento, caso se verifique a conformidade da proposta de que trata o subitem 6.6, o pregoeiro passará à verificação da documentação de habilitação do licitante conforme disposições do item 7.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas pormenorizadas neste Edital ou em seus Anexos;

6.7.3. apresentar preços inexequíveis ou permanecer acima do preço máximo definido para a contratação;

6.7.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus Anexos, desde que insanável.

6.8. Serão considerados indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o subitem anterior, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o licitante comprove a exequibilidade da proposta.

6.10. Erros no preenchimento de planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

6.10.1. O ajuste de que trata o subitem anterior se limita a sanar erros ou falhas que não alterem a substância das propostas.

6.10.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

6.11. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos que serão exigidos para fins de habilitação estão especificados na documentação que constitui Anexo deste Edital, consistindo na documentação necessária e suficiente para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.1.2. Nesta licitação, não haverá exigência de que o licitante ateste, sob pena de inabilitação, que conhece o local e as condições de realização do objeto, ou que tem conhecimento pleno das condições e peculiaridades da contratação.

7.1.3. Para pessoas jurídicas em consórcio, será admitido o somatório dos quantitativos de cada consorciado para efeito de habilitação técnica e, para efeito de habilitação econômico-financeira, será admitido o somatório dos valores de cada consorciado.

7.1.3.1. Para a comprovação da exigência dos requisitos de habilitação econômico-financeira das pessoas jurídicas em consórcio, conforme subitem anterior, haverá um acréscimo de 10% (dez por cento) para o consórcio em relação ao valor exigido dos licitantes individuais para habilitação econômico-financeira, salvo se o consórcio for formado integralmente por microempresas ou empresas de pequeno porte.

7.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

7.3. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133, de 2021.

7.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133, de 2021).

7.5. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que 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.

7.6. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.7. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.7.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 4º, § 1º, e art. 6º, § 4º, c/c Decreto estadual nº 67.608, de 2023).

7.8. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, *caput*, c/c Decreto estadual nº 67.608, de 2023).

7.8.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação. (Instrução Normativa SEGES/MPDG nº 3, de 2018, art. 7º, parágrafo único, c/c Decreto estadual nº 67.608, de 2023).

7.9. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 2 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

7.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.10.1. Os documentos relativos à regularidade fiscal especificados na documentação que integra este Edital como Anexo somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.11. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei nº 14.133, de 2021, art. 64):

7.11.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.11.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.12. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.13. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente Edital, observado o prazo definido no subitem 7.9.1.

7.14. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao Edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.15. A comprovação de regularidade fiscal e trabalhista das microempresas, das empresas de pequeno porte e das cooperativas que atendam ao disposto no art. 34 da Lei n° 11.488, de 2007 somente será exigida para efeito de contratação, e não como condição para participação na licitação.

7.15.1. Havendo alguma restrição no que tange à regularidade fiscal e trabalhista, o licitante habilitado nas condições do subitem anterior deverá comprovar sua regularização sob pena de decadência, sem prejuízo da aplicação das sanções cabíveis, mediante a apresentação

das competentes certidões negativas de débitos, ou positivas com efeito de negativa, no prazo de 5 (cinco) dias úteis, contado a partir do momento em que o licitante for declarado vencedor do certame, prorrogável por igual período, a critério da Administração.

7.16. A disciplina da adjudicação, da homologação e da contratação encontra-se no item 11 deste Edital.

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.2. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos;

8.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar o recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados pelo sistema SEI/SP.

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante ou contratado que, com dolo ou culpa:

9.1.1. der causa à inexecução parcial do contrato;

9.1.2. der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.1.3. der causa à inexecução total do contrato;

9.1.4. deixar de entregar a documentação exigida para o certame, inclusive não entregar qualquer documento que tenha sido solicitado pelo pregoeiro durante o certame;

9.1.5. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

9.1.5.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.5.2. recusar-se a enviar o detalhamento da proposta quando exigível; ou

9.1.5.3. pedir para ser desclassificado quando encerrada a etapa competitiva.

9.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.6.1. recusar-se, sem justificativa, a formalizar a contratação no prazo e condições estabelecidos pela Administração;

9.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

9.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

9.1.9. fraudar a licitação ou praticar ato fraudulento na execução do contrato;

9.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.10.1. agir em conluio ou em desconformidade com a lei;

9.1.10.2. induzir deliberadamente a erro no julgamento;

9.1.11. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

9.1.12. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fundamento na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes, adjudicatários e/ou contratado as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar; e

9.2.4. declaração de inidoneidade para licitar ou contratar.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida;

9.3.2. as peculiaridades do caso concreto;

9.3.3. as circunstâncias agravantes ou atenuantes;

9.3.4. os danos que dela provierem para a Administração Pública;

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A sanção de multa será calculada em conformidade com o Regulamento Anexo à Portaria Normativa nº 444/2024, que integra este instrumento, e aplicada após regular processo administrativo.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a penalidade de multa, garantido o exercício de prévia e ampla defesa.

9.6. A sanção de advertência será aplicada, após regular processo administrativo, ao responsável em decorrência da infração administrativa relacionada no subitem 9.1.1, quando não se justificar a imposição de penalidade mais grave.

9.7. A sanção de impedimento de licitar e contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos subitens 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6 e 9.1.7, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do Estado de São Paulo, pelo prazo máximo de 3 (três) anos.

9.8. A sanção de declaração de inidoneidade para licitar ou contratar será aplicada, após regular processo administrativo, ao responsável em decorrência das infrações administrativas relacionadas nos subitens 9.1.8, 9.1.9, 9.1.10, 9.1.11 e 9.1.12, bem como das infrações administrativas previstas nos subitens 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6 e 9.1.7 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja extensão e duração observará o prazo previsto no art. 156, § 5º, da Lei n.º 14.133, de 2021.

9.9. A recusa injustificada do adjudicatário em formalizar a contratação no prazo e condições estabelecidos pela Administração, descrita no subitem 9.1.6.1, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas (art. 90, § 5º, da Lei nº 14.133, de 2021).

9.10. Os procedimentos para apuração e aplicação das sanções administrativas relacionadas à presente licitação estão previstos no Regulamento Anexo à Portaria Normativa nº 444/2024, que integra este instrumento.

9.11. As sanções são autônomas e a aplicação de uma não exclui a de outra.

9.12. A aplicação das sanções previstas neste Edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados à Administração Pública.

9.13. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante à Contratada, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra o Edital, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

9.14. Os atos previstos como infrações administrativas na lei de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013,

serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei.

9.15. A personalidade jurídica poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, nos termos do art. 160 do referido diploma legal.

9.16. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo federal (art. 161 da Lei nº 14.133, de 2021).

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, ou para solicitar esclarecimento sobre os seus termos, devendo protocolar a impugnação ou o pedido de esclarecimento até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, *pelo seguinte meio*: *slicp@fundacaocasa.sp.gov.br*.

10.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.3.1. A concessão de efeito suspensivo à impugnação é medida excepcional, e, caso ocorra, será motivada nos autos do processo de licitação.

10.4. A decisão da impugnação ou a resposta ao pedido de esclarecimento serão divulgadas em sítio eletrônico oficial conforme especificado no subitem subsequente, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.4.1. As decisões das impugnações e as respostas aos pedidos de esclarecimento serão juntadas aos autos do processo licitatório, ficarão disponíveis para consulta por qualquer interessado, e serão publicadas *no sistema e no endereço eletrônico na Internet www.fundacaocasa.sp.gov.br, opção Transparência*, sem informar a identidade do responsável pela impugnação ou pelo pedido de esclarecimento.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando a alteração não comprometer a formulação das propostas.

10.6. A ausência de impugnação implicará na aceitação tácita, pelo licitante, das condições previstas neste Edital e em seus Anexos.

10.7. A ausência de pedido de esclarecimento implicará na presunção de que os interessados não tiveram dúvidas a respeito da presente licitação, razão pela qual não serão admitidos questionamentos extemporâneos.

11. DAS DISPOSIÇÕES GERAIS

11.1. Exaurida a fase recursal, será observado o disposto no art. 71 da Lei nº 14.133, de 2021.

11.2. Constatada a regularidade dos atos praticados, a autoridade superior adjudicará o objeto da licitação ao licitante vencedor e homologará o procedimento licitatório.

11.2.1. Após a homologação da licitação, em sendo realizada a contratação, sua formalização ocorrerá mediante a assinatura de termo de contrato, cuja minuta integra este Edital como Anexo.

11.2.1.1. Se, por ocasião da formalização da contratação, algum dos documentos apresentados pelo adjudicatário para fins de comprovação das condições de

habilitação estiver com o prazo de validade expirado, a Administração verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando a ele os documentos comprobatórios, salvo impossibilidade devidamente justificada.

11.2.1.2. Se não for possível atualizar os documentos referidos no subitem anterior por meio eletrônico hábil de informações, o adjudicatário será notificado 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.

11.2.1.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome do adjudicatário no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL". Esta condição será considerada cumprida se o devedor comprovar que os respectivos registros se encontram suspensos, nos termos do art. 8º, §§ 1º e 2º, da Lei estadual nº 12.799, de 2008.

11.2.1.4. Com a finalidade de verificar se o licitante mantém as condições de participação no certame, serão novamente consultados, previamente à celebração da contratação, os cadastros especificados no item 6.1 deste Edital.

11.2.2. Constitui(em), igualmente, condição(ões) para a celebração da contratação:

11.2.2.1. a apresentação do(s) documento(s) que o adjudicatário, à época do certame licitatório, houver se comprometido a exibir por ocasião da celebração da contratação por meio de declaração específica, caso exigida na documentação que integra este Edital como Anexo;

11.2.2.2. a indicação de gestor encarregado de representar o adjudicatário com exclusividade perante o contratante, caso se trate de sociedade cooperativa.

11.2.3. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decadência do direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

11.2.3.1. O contrato será assinado com a utilização de meio eletrônico, nos termos da legislação aplicável.

11.2.3.2. O prazo para assinatura previsto no subitem anterior poderá ser prorrogado por igual período, por solicitação justificada do interessado e aceita pela Administração.

11.2.3.3. Será considerado celebrado o contrato, em caso de assinaturas por meio eletrônico em datas diferentes, na data da última assinatura eletrônica das partes do termo contratual.

11.2.4. Na hipótese de o vencedor da licitação não comprovar manter as condições de habilitação e preencher as condições de contratação consignadas neste Edital, ou não assinar o contrato, ou recusar a contratação, a Administração, sem prejuízo da apuração do cabimento de aplicação de sanções e das demais cominações legais cabíveis a esse licitante, poderá convocar os licitantes remanescentes, respeitada a ordem de classificação, para a celebração do contrato em conformidade com o procedimento e as condições estabelecidas no art. 90 da Lei nº 14.133, de 2021.

11.2.5. Será facultada à Administração a convocação dos demais licitantes classificados para a contratação de remanescente em consequência de rescisão de contrato celebrado com fundamento nesta licitação, observados os critérios estabelecidos no § 7º do art. 90 da Lei nº 14.133, de 2021.

11.3. Será divulgada ata da sessão pública no sistema eletrônico.

11.4. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo pregoeiro.

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

11.6. A homologação do resultado desta licitação não implicará direito à contratação.

11.7. As normas disciplinadoras da licitação serão interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse público, o princípio da isonomia, a finalidade e a segurança da contratação.

11.8. Os casos omissos serão solucionados pelo pregoeiro.

11.9. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.10. 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 na Administração.

11.11. No julgamento das propostas e da habilitação, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

11.11.1. As falhas passíveis de saneamento na documentação apresentada pelo licitante são aquelas cujo conteúdo retrate situação fática ou jurídica já existente na data da abertura da sessão pública deste Pregão.

11.11.2. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público, nos termos do inciso III do art. 12 da Lei nº 14.133, de 2021.

11.12. Caso seja vencedor da licitação, o licitante a ser contratado estará sujeito à assinatura de Termo de Ciência e de Notificação, quando prevista a sua apresentação em ato normativo editado pelo Tribunal de Contas do Estado de São Paulo, conforme a disciplina aplicável.

11.13. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e nos endereços eletrônico *www.fundacaocasa.sp.gov.br, opção Transparência e www.imprensaoficial.com.br, opção e-negociospublicos.*

11.14. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado de São Paulo.

11.15. Integram este Edital, para todos os fins e efeitos, os seguintes Anexos:

11.15.1. Termo de Referência – Anexo I do Edital;

11.15.1.1. Estudo Técnico Preliminar – Anexo do Termo de Referência;

11.15.2. Minuta de Contrato - Anexo II do Edital;

11.15.3. Cópia do Regulamento Anexo à Portaria Normativa nº 444/2024 - Anexo III do Edital;

11.15.4. Modelo referente a planilha de proposta - Anexo IV do Edital;

11.15.5. Modelo de Declaração exigida para Habilitação - Anexo V do Edital.

São Paulo, 21 de maio de 2025.

Magda de Oliveira Vieira
Diretor de Divisão Interino

ANEXO I

Termo de Referência 60/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
60/2025	990202-ESP-FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO	DENISE VITIRITO DE OLIVEIRA	20/05/2025 18:56 (v 9.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
I - alienação e concessão de direito real de uso de bens/Alienação		161.00039823/2025-01

1. Condições gerais da contratação

1.1. Contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	QTD	UNIDADE DE MEDIDA	ESPECIFICAÇÃO	CATSER	CÓD. SIAFISICO
1	1	Unidade	Serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter.	27090	39187

1.1.1. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.1.2. Este Termo de Referência foi elaborado em conformidade com o Decreto estadual nº 68.185, de 11 de dezembro de 2023.

1.1.3. O objeto desta contratação não se enquadra como serviços de luxo, observando o disposto no Decreto estadual nº 67.985, de 27 de setembro de 2023.

1.1.4. Considerando o valor estimado para a contratação, a presente licitação será de participação ampla, sendo aplicáveis as regras de tratamento favorecido constantes dos arts. 42 a 45 da Lei Complementar nº 123, de 2006, observado o disposto no § 2º do art. 4º da Lei nº 14.133, de 2021.

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar, elaborado nos termos do Decreto estadual nº 68.017, de 11 de outubro de 2023.

1.3. O(s) serviço(s) objeto desta contratação é enquadrado como contínuo, sem regime de dedicação exclusiva de mão de obra e sem predominância de mão de obra, tendo em vista a natureza da prestação em questão.

1.4. O prazo de vigência da contratação é de 12 (doze) meses, contados da data estabelecida para início dos serviços, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

Subcontratação

1.5. O Contratado não poderá subcontratar, ceder ou transferir, total ou parcialmente, o objeto contratual.

Validade da proposta

1.6. Para garantir a estabilidade da proposta e permitir a análise adequada do processo, especialmente em licitações mais complexas, a validade não será inferior a 180 (cento e oitenta) dias, a contar da data de sua apresentação.

1.6.1. Ressaltamos que esse prazo não traz custos extras aos fornecedores, uma vez que define um período razoável para a validade da proposta, seguindo as práticas do mercado, evitando retrabalho e assegurando a continuidade do certame sem prejuízos à Administração.

2. Descrição da solução

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3. Fundamentação e descrição da necessidade

3.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.3. O objeto da contratação está previsto no Plano de Contratações Anual 2024, que será executado em 2025, nos termos do Decreto Estadual nº 67.689, de 3 de maio de 2023, e segue divulgado no Portal Nacional de Contratações Públicas (PNPC) e no site institucional da Fundação Casa. A consulta ao PCA-2025 pode ser realizada através do link de acesso: https://fundacaocasa.sp.gov.br/index.php/plano-de-contratacao-anual/.

4. Requisitos da contratação

Requisitos de Negócio

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. Os itens a serem contratados serão licitados em apenas uma solução, prestados por uma única empresa visando a racionalização e gestão com ampla definição de responsabilidade em caso de acionamento da garantia, tendo em vista que todo o sistema tem grande complexidade, evitando-se comprometer a efetividade do serviço prestado.

4.1.2. Em virtude da complexidade do ambiente e da criticidade das aplicações existentes e em produção, os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte A, deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

4.1.3. Os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte B, poderão ser prestados diretamente pelo próprio fabricante correlacionado ao produto (Dell, IBM, HP, Fortinet, etc.) ou por seus parceiros autorizados.

4.1.4. Os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware e Fortigate listados na tabela – parte C, deverão ser prestados pelo próprio fabricante (Vmware e Fortinet) para todas as licenças existentes na Fundação Casa.

4.1.5. A fim de manter a qualidade dos serviços prestados para a Fundação Casa, caso haja a necessidade a CONTRATANTE poderá solicitar a substituição de qualquer equipamento listado na tabela, partes A e C, por um equipamento novo desde que se encontre em linha de produção e sem uso anterior devidamente aprovado pela equipe técnica da Fundação Casa. Este equipamento deverá ter performance igual ou superior ao já existente e deverá possuir garantia direta pelo fabricante do produto.

4.2. DA PRESTAÇÃO DO SERVIÇO

4.2.1. Visando conhecer o ambiente da CONTRATANTE, no início da vigência do contrato, em período a ser agendado, será realizada a etapa de OPERAÇÃO ASSISTIDA, na qual, durante no mínimo de 30 (trinta) dias, a CONTRATADA analisará e fornecerá, à CONTRATANTE, informações sobre a conformidade do ambiente (Configuração e Desempenho), no que tange a aplicação de atualização de SOFTWARE e HARDWARE.
4.2.2. O fornecimento das informações coletadas e analisadas deverá ocorrer em até 5 (cinco) dias após término da atividade de OPERAÇÃO ASSISTIDA.
4.2.3. A CONTRATADA se compromete a manter em correto e adequado funcionamento o “ambiente de processamento e armazenamento atual”, indicado no item 2, através da realização de SUPORTE TÉCNICO à CONTRATANTE.
4.2.4. A CONTRATADA atuará no “ambiente de processamento e armazenamento Dell”, tanto no HARDWARE quanto a SOFTWARE, realizando a aplicação de atualizações que vierem a ser disponibilizadas pelas fabricantes e a troca de itens que apresentem falha no decorrer do contrato.
4.2.5. O SUPORTE TÉCNICO ocorrerá em resposta à abertura de CHAMADO TÉCNICO realizada pela CONTRATANTE ou quando for detectada a necessidade de atuação no ambiente da CONTRATANTE, como, por exemplo, nos casos em que o fabricante disponibiliza um novo pacote de correção de erros.
4.2.6. A abertura de CHAMADO TÉCNICO pela CONTRATANTE será realizada por meio de ligação telefônica, envio de mensagem eletrônica ou registro em sistema próprio da CONTRATADA.
4.2.7. Cada CHAMADO TÉCNICO deverá receber identificação única e inequívoca.
4.2.8. Não deverá haver limitação quanto ao número de CHAMADOS TÉCNICOS que podem ser

abertos.

4.2.9. A existência de um CHAMADO TÉCNICO, independentemente da sua fase de atendimento, não deverá restringir a abertura de novos CHAMADOS TÉCNICOS.

4.2.10. A abertura de um novo CHAMADO TÉCNICO não implica no consequente encerramento de qualquer outro CHAMADO TÉCNICO.

4.2.11. A CONTRATADA deverá monitorar o envio de alertas pelos equipamentos do ambiente para, nos casos de envio de alerta, proceder à abertura de CHAMADO TÉCNICO.

4.2.12. Abertura de CHAMADO TÉCNICO e ATENDIMENTO TÉCNICO deverão estar disponíveis em regime 24x7 (24 horas por dia e 7 dias da semana).

4.2.13. As atividades de ATENDIMENTO TÉCNICO deverão ser realizadas por técnico da CONTRATADA e serão acompanhadas pela CONTRATANTE, devendo ser previamente agendadas.

4.2.14. Para os casos em que haja necessidade de interrupção dos serviços, mesmo que de forma parcial, o tempo total de indisponibilidade não deverá exceder 4 (quatro) horas.

4.2.15. Salvo manifestação contrária da CONTRATANTE, as atividades de atendimento técnico deverão ser realizadas presencialmente e fora do horário comercial.

4.2.16. A CONTRATADA deverá proceder ao atendimento dos CHAMADOS TÉCNICOS abertos observando os seguintes critérios:

4.2.17. Em até 2 horas da abertura, analista ou técnico da CONTRATADA deverá contatar a equipe da CONTRATANTE visando melhor entendimento do chamado, do estado do ambiente e, principalmente, para posicionar a equipe da CONTRATANTE sobre o procedimento que será executado pela CONTRATADA.

4.2.18. Em até 6 horas da abertura, para situações em que o ambiente esteja com o DESEMPENHO DEGRADADO ou em ESTADO CRÍTICO a CONTRATADA deverá proceder ao atendimento e conclusão do CHAMADO TÉCNICO, restaurando o ambiente ao seu modo normal de operação.

4.2.19. Para situações em que o ambiente não esteja em estado crítico ou com desempenho degradado a CONTRATADA disporá de 24 horas para atendimento e finalização do CHAMADO TÉCNICO.

4.2.20. A CONTRATADA deverá realizar visitas técnicas preventivas ao ambiente onde os equipamentos estão instalados. Estas visitas presenciais deverão ter periodicidade mínima mensal com duração mínima de 4 horas, podendo ser distribuídas entre as localidades, em dias úteis, de forma a verificar logs, mensagens de erros e eventuais atualizações de software ou correções preventivas.

4.2.21. A CONTRATADA deverá disponibilizar atendimento em língua portuguesa, sendo aceito para documentos que termos e textos técnicos poderão estar na língua inglesa.

4.2.22. Exceto para os casos de atualização e mudança de versão, quando detectada a necessidade de substituição de algum SOFTWARE a CONTRATADA deverá fornecer outro SOFTWARE que cumpra minimamente as funcionalidades daquele substituído.

4.2.23. O SOFTWARE, suas licenças e itens que este necessite deverão ser fornecidos objetivando o correto funcionamento e licenciamento do ambiente da CONTRATANTE.

4.2.24. A CONTRATADA deverá providenciar a renovação do suporte técnico oficial de todas as licenças de software de gerenciamento centralizado de virtualização do fabricante Vmware, conforme quantitativo do ANEXO I, listagem de softwares – Parte C, durante a vigência do contrato.

4.2.25. A CONTRATADA deverá providenciar a renovação do suporte técnico oficial e de todas as licenças de software de gerenciamento centralizado de virtualização do fabricante Fortigate, conforme quantitativo do ANEXO I, listagem de softwares – Parte C, durante a vigência do contrato.

4.2.26. Caso a CONTRATANTE identifique a necessidade de treinamento, devido a mudança do modo de operação do ambiente ou em decorrência da substituição, atualização ou upgrade de qualquer software utilizado pela CONTRATANTE, a CONTRATADA deverá providenciá-lo, em 2 turmas distintas, de modo a capacitar a equipe da CONTRATANTE a operar o novo SOFTWARE disponibilizado.

4.2.27. Detectada a necessidade de substituição de alguma PEÇA, esta deverá ser substituída

por uma peça nova, original e sem uso anterior.

4.2.28. Caso a substituição da PEÇA ocorra e haja necessidade de substituição de algum SOFTWARE, está substituição será de responsabilidade da CONTRATADA, devendo ser observadas e obedecidas as condições estabelecidas para os casos de substituição de SOFTWARE.

4.2.29. Sempre que for identificada a necessidade de substituição de algum item, independentemente deste representar uma PEÇA ou SOFTWARE, a CONTRATADA deverá obter a anuência formal do CONTRATANTE para a substituição pretendida.

4.2.30. A CONTRATANTE se reserva o direito de exigir a substituição dos equipamentos em definitivo por outro, com as mesmas características e capacidade, quando o mesmo apresentar repetidamente, máximo de 3 vezes, em 90 (noventa) dias, os mesmos defeitos durante a vigência do contrato. Caso a CONTRATANTE solicite a substituição de um determinado equipamento de hardware, o equipamento a ser entregue pela CONTRATADA deverá ser novo, sem uso anterior e com as especificações técnicas iguais ou superiores ao equipamento substituído.

4.2.31. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do Departamento de Tecnologia da Informação - DTI, referentes a qualquer problema detectado ou ao andamento de atividades de suporte técnico previstas.

4.2.32. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Fundação Casa ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

4.2.33. Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do(s) serviço(s) e o atendimento às especificações contidas no Contrato, Edital e em seus Anexos.

4.2.34. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato de Prestação de Serviço, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridas.

4.2.35. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina da repartição ou ao interesse do serviço público, sempre que exigido pelo Gestor do Contrato do Departamento de Tecnologia da Informação.

4.2.36. Comunicar, formal e imediatamente ao Gestor do Contrato, todas as ocorrências anormais e/ou que possam comprometer a execução dos serviços contratados.

4.2.37. Entregar mensalmente, para fins de controle, relatório de prestação de serviço de suporte técnico realizado no período. Deverão constar, no mínimo, as seguintes informações:

4.2.38. Relação de todos os chamados técnicos ocorridos no período, incluindo data e hora do início e término do atendimento.

4.2.39. Identificação do problema; severidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva

4.2.40. Data e hora do início e término da solução definitiva.

4.2.41. Identificação dos técnicos do Departamento Tecnologia Informação - DTI, que solicitou e validou o chamado.

4.2.42. Identificação do técnico do Fornecedor responsável pela execução do chamado, bem como outras informações pertinentes.

4.2.43. Prestar suporte técnico a todas as funcionalidades presentes e necessárias para o pleno estado de funcionamento dos equipamentos.

4.2.44. Manter sigilo sobre todo e qualquer assunto de interesse da Fundação CASA, ou de terceiros, de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

4.2.45. Responder pela reparação dos danos causados por defeitos relativos aos serviços prestados. Por isso deverá prezar pela qualidade e eficiência, garantindo que os serviços e também

as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo Departamento Tecnologia Informação – DTI, quando da abertura dos chamados técnicos.

4.2.46. A CONTRATANTE se reserva o direito de exigir da CONTRATADA, a seu único critério e a qualquer tempo durante a vigência do contrato, que alguns dos componentes considerados importantes, necessários e estratégicos para a execução deste contrato, como HD's, fontes e ventiladores, sejam armazenados no ambiente da CONTRATANTE durante a vigência do contrato, de forma a ser utilizada de maneira emergencial em caso de necessidade. Caso seja solicitada pela CONTRATANTE esse armazenamento local, as peças não utilizadas serão devolvidas à CONTRATADA ao término do contrato.

4.2.47. Deverão ser fornecidos, nas periodicidades abaixo indicadas, relatórios de acompanhamento com as seguintes características:

4.2.48. Reportar o número de CHAMADOS TÉCNICOS em aberto ou em atendimento, e CHAMADOS TÉCNICOS concluídos no mês anterior.

4.2.49. Descrição do motivo da abertura do CHAMADO TÉCNICO e descrição da solução, se concluído.

4.2.50. Periodicidade quadrimestral: Indicar as atualizações de hardware e software que necessitam ser aplicadas no ambiente.

4.2.51. A CONTRATADA deverá manter o sigilo de documentos e informações da CONTRATANTE a que eventualmente tenha acesso.

4.3. DO MONITORAMENTO DO AMBIENTE

4.3.1. A CONTRATADA deverá fornecer, implementar e suportar um serviço de monitoramento através de um centro de monitoramento de redes (NOC), capaz de monitorar os equipamentos do ambiente da CONTRATANTE, acompanhar alertas, , com no mínimo as seguintes características:

4.3.2. Solução de monitoramento utilizando dispositivo de hardware dedicado a função de monitoramento de infraestrutura, não sendo aceito soluções montadas sob a plataforma PC/x86 nem dispositivos montados usando soluções Open Source.

4.3.3. Deve permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

4.3.4. Deve possuir, no máximo, 1 RU (Rack Unit) de altura.

4.3.5. Deve possuir 2 fontes de alimentação AC bivolt interna, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).

4.3.6. Processador interno com quatro cores, Intel x86 ou equivalente, para permitir execução de aplicações internas tipo Dockers ou Kubernetes

4.3.7. Deve possuir 16 portas seriais com suporte a expansão até 96 portas seriais com conectores seriais RJ-45 em uma unidade "RU", sem a utilização de switches externos

4.3.8. Deve possuir para up-link ou aceso, no mínimo, 2 (duas) portas Gigabit Ethernet (10/100 /1000BT) com interface RJ-45 e 2 (duas) portas SFP+ 10GB.

4.3.9. Deve permitir alimentação de energia em corrente contínua (DC).

4.3.10. Deve possuir portas tipo USB para conectar modem celular, serial, ethernet, Wi-Fi, armazenamento e modem analógico e ou ethernet via conversor USB-Ethernet.

4.3.11. Deve permitir o acesso opcional via rede móvel LTE 5G/4G, devendo ser fornecido com chip de dados ativo;

4.3.12. Permitir acesso pelos protocolos HTTPS, SSHv2; opcional HTTP, Telnet and SSHv1.

4.3.13. Permitir a configuração via interface Gráfica ou linha de comando e Linux.

4.3.14. Deve suportar no mínimo 32GB de armazenamento interno.

4.3.15. Deve suportar as funções de servidor DHCP e executar roteamento e funções de firewall.

4.3.16. Deve suportar plataforma para Automação para end device via Python Scripts, Puppet, Chef, Docker e Ansible

4.3.17. Deve suportar automação via diferentes meios, incluindo, shell Script, Cloud, RESTFUL, ANSIBLE, Chef, Docker, KVM Hypervisor, Puppet, Python, RedHat Ansible, Ruby, Node.js JavaScript

4.3.18. Permitir Agrupamento de equipamentos via software em grupos associando múltiplas

unidades e permitir o gerenciamento através do login em uma das unidades apenas.
4.3.19. Envio de alertas e eventos deve permitir envio de mensagens via log de sistema, E-mail e na própria console.
4.3.20. Deve suportar a customização do nível de acesso de usuários.
4.3.21. Deve suportar a descoberta automática de novos dispositivos.
4.3.22. Deve permitir configurar suporte a NTP, zonas de horários mundiais ou sincronização através de torre de celular.
4.3.23. Deve permitir a restrição do acesso à interface de linha de comando (CLI) através de senha e dupla autenticação usando protocolos RSA e DUO.
4.3.24. Deve permite NAT e possuir funções de Firewall integrado com o sistema operacional. Deve suportar tunelamento através de SSL VPN, IPSec e Wireguard VPN.
4.3.25. Deve suportar mecanismos de AAA (Authentication, Authorization e Accounting), com suporte aos protocolos RADIUS e TACACS+, LDAP e Kerberos
4.3.26. Deve suportar o protoco IPv6;
4.3.27. Deve permitir a configuração de endereços IPv6 para gerenciamento;
4.3.28. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;
4.3.29. Deve suportar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;
4.3.30. Deve suportar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6\ Suportar IPv4 / IPv6.

4.3.31. Solução para contingência e quarentena de arquivos potencionamente maliciosos;

4.3.32. O ambiente disponibilizado tem como finalidade testar e analisar arquivos potencialmente maliciosos em um ambiente seguro, controlado e isolado. Deverá permitir a execução de arquivos suspeitos, monitorando seu comportamento e suas interações com o sistema para detectar atividades maliciosas, como tentativas de explorar vulnerabilidades, modificações no sistema ou comunicação com servidores externos.
4.3.33. O ambiente deverá ser completamente isolado da rede corporativa e de sistemas de produção, prevenindo qualquer propagação de malware ou impactos negativos nos sistemas reais.
4.3.34. O ambiente deverá simular sistemas operacionais completos e redes de comunicação para capturar todas as ações realizadas pelo arquivo em teste.
4.3.35. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.

4.4. CARACTERISTICAS DA SOLUÇÃO DE CLOUD COMPUTING

4.4.1. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.
4.4.2. Todos os equipamentos de hardware e software utilizados para a prestação de serviços devem ser de propriedade da licitante, que deverá ser responsável pela operação e manutenção dos equipamentos, não sendo permitida a revenda ou intermediação de serviços de terceiros.
4.4.3. A Contratada deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para a CONTRATADA, de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, a partir de seu Centro de

Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana).

4.4.4. A solução de Computação em Nuvem ofertada deve permitir a criação de uma ou mais VPC´s (Virtual Private Cloud), de forma que a CONTRATADA possa provisionar uma seção da nuvem da solução ofertada isolada logicamente, onde é possível executar recursos da solução em uma rede virtual definida pela CONTRATADA, permitindo o controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub redes e a configuração de tabelas de rotas e gateways de rede, para acessar recursos e aplicações com segurança e facilidade. Além disso, a CONTRATADA poderá criar uma conexão de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e a VPC e aproveitar a nuvem da solução ofertada como uma extensão do seu datacenter corporativo.

4.4.5. A solução deverá ser escalável, de forma a permitir aumentar os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver a demanda complementar oriunda de picos de acesso ou expansão natural dos usuários em ambiente Cloud Computing.

4.4.6. Os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

4.4.7. Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco.

4.4.8. Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente físico.

4.4.9. É de responsabilidade da Contratada o monitoramento do hardware e seus componentes, bem como a manutenção dos mesmos, identificando necessidades de reposições, adaptações e melhorias, procedendo chamados aos fornecedores, acompanhando, garantindo a devida solução aos problemas que porventura ocorram, observando os tempos definidos no Nível de Serviço Exigido e fornecendo Console de Gestão para monitoramento em tempo real de todos os recursos computacionais.

4.4.10. O monitoramento deverá ser feito de forma continuada, não sobrecarregando os equipamentos ou consumindo recursos da solução de cloud computing provisionada aos clientes.

4.4.11. CARACTERISTICAS DA INFRAESTRUTURA FÍSICA

4.4.11.1. A solução proposta deverá hospedar os dados em datacenter localizado em território nacional;

4.4.11.2. Para fins de segurança da informação os dados deverão ser replicados entre datacenters com no mínimo 40km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica.

4.4.11.3. Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Datacenter, que deverá manter compatibilidade com padrões internacionais, e deverão manter compatibilidade durante toda vigência do contrato.

4.4.11.4. As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviço atenderão, no mínimo, às características aqui definidas de estrutura física, instalações físicas, energia elétrica, climatização, proteção contra incêndio, segurança física, infraestrutura de acesso à internet do Datacenter e segurança lógica do Datacenter.

4.4.11.5. Os datacenters da CONTRATADA deverão possuir um ambiente com alta disponibilidade, atendendo aos seguintes requisitos mínimos:

4.4.11.5.1. Possuir certificação padrão TIER III;

4.4.11.5.2. Possuir no mínimo as seguintes certificações:

4.4.11.5.3. Garantir a disponibilidade imediata de energia elétrica através do fornecimento de sistemas de nobreaks independentes e redundantes

4.4.11.6. Redundância no fornecimento de portas de rede de acesso, através da disponibilidade de no mínimo dois switches distintos e independentes com portas Gigabit Ethernet ou superior com ao menos duas portas disponíveis em cada switch.

4.4.11.7. A fim de se comprovar o atendimento à estes requisitos mínimos, a CONTRATANTE se reserva o direito de realizar uma vistoria técnica presencial no ambiente da CONTRATADA, a

qualquer momento durante a vigência deste contrato, mediante agendamento prévio.
4.4.11.8. Caso ocorram quaisquer despesas de deslocamento ou viagem para a realização desta vistoria presencial, as despesas serão de responsabilidade da CONTRATADA.

4.4.12. CONSOLE DE GESTÃO DO AMBIENTE CLOUD COMPUTING

4.4.12.1. Permitir o gerenciamento da infraestrutura de Computação em Nuvem de forma independente de softwares de cliente (VNC, Remote Desktop, SSH, etc), por meio de API (Application Programming Interface), acessada via browser, de forma segura (HTTPS), utilizando-se de recursos de autenticação.
4.4.12.2. O acesso via interface web browser não poderá permitir a visualização ou edição de qualquer componente persistente a infraestrutura física que compõe a solução.
4.4.12.3. Possibilitar o cadastramento dos colaboradores da CONTRATANTE, inclusive, por perfil de acesso para administrar, operar ou consultar o ambiente de produção da solução na infraestrutura de Computação em Nuvem disponibilizada pela CONTRATADA.
4.4.12.4. Permitir selecionar modelos preexistentes (templates) de máquinas virtuais e sistemas operacionais.
4.4.12.5. Permitir personalizar modelos (templates) que melhor se adaptem às necessidades da CONTRATANTE.
4.4.12.6. Permitir modificar os recursos da Infraestrutura de Computação em Nuvem e atualizá-los de uma forma controlada e previsível, aplicando-se, quando necessário, controles de versionamento, devendo ser permitido o rastreamento das alterações históricas efetuadas no ambiente.
4.4.12.7. Disponibilizar console via interface gráfica afim de permitir o agendamento, realização de backups e horários de funcionamento por recurso (servidor; banco de dados, fileserver), por ambiente (produção) ou por etiqueta (classificação das soluções/sistemas).
4.4.12.8. Deverá ser disponibilizado um painel de controle (software de gestão para alojamento web) com as opções mínimas de: gerenciamento FTP, gerenciamento de arquivos, gerenciamento de banco de dados, verificação de estatísticas, gerenciamento de domínios;
4.4.12.9. Conexão a 2 pontos de troca de trafego distintos;
4.4.12.10. Deverá possuir gerenciador de arquivos web;
4.4.12.11. Deverá possuir painel de gerenciamento de DNS.

4.4.13. MONITORAMENTO DE RECURSOS

4.4.13.1. A Contratada deverá oferecer Console de Gestão de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Computação em Nuvem por meio de web browsers.
4.4.13.2. A solução ofertada deverá permitir o monitoramento das máquinas virtuais, provendo o monitoramento do ambiente de Computação em Nuvem (serviços e recursos), de forma automatizada e abrangendo servidores, sistemas operacionais e recursos de comunicação, em tempo real (24x7x365), visando detectar problemas (incidentes), no que tange à sustentação operacional e não a aplicação do Contratante.
4.4.13.3. Prover o monitoramento constante em amostras com granularidade mínima de 1 hora (24X7X365) dos serviços e recursos, visando detectar os problemas mais frequentes, informando a CONTRATANTE a ocorrência destes.
4.4.13.4. Deverá ser realizada pela Contratada a monitoração da qualidade e nível de utilização da infraestrutura de acesso à Internet, disponibilizada pela solução ofertada pela Contratada, bem como as resoluções em caso de problemas.
4.4.13.5. Deverá permitir a visualização dos indicadores de desempenho, falhas do ambiente e características e requisitos operacionais dos recursos gerenciados por meio do painel de apresentação (dashboard) Online (tempo real).
4.4.13.6. A solução ofertada deverá prover alarmes para a Console de Gestão de eventos,

mostrando quais recursos estiveram acima do threshold, permitindo gerar relatório a partir dos eventos observados.
4.4.13.7. Para cada servidor virtual, deverá ser possível o acompanhamento e monitoramento dos seguintes recursos: vCPU, RAM, Tráfego de Rede (In/Out) e Disco.

4.4.14. SERVIDORES VIRTUALIZADOS E RECURSOS COMPUTACIONAIS

4.4.14.1. Todos os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:
4.4.14.2. Implementar características de escalabilidade vertical (aumento/diminuição de recursos do mesmo servidor), incluindo flexibilidade de configuração de memória, processador e disco;
4.4.14.3. Permitir a criação, pela CONTRATANTE, de pelo menos 1 (uma) imagem (snapshot) dos servidores virtuais sem custo adicional;
4.4.14.4. Assegurar a comunicação segura e encriptada entre os próprios servidores e os clientes que farão acesso aos mesmos, através de protocolo seguro HTTPS, ou seja, todos os servidores deverão ser disponibilizados com certificados digitais SSL instalados.
4.4.14.5. Os recursos computacionais adicionais, poderão ser utilizados para agregação ou distribuição entre os servidores virtualizados existentes ou para a criação de novos servidores virtuais;
4.4.14.6. Deverá ser considerado um pool de recursos computacionais para suprir a demanda de todas as máquinas virtuais do ambiente atualmente em produção e no mínimo com as seguintes características Processador e Memória.
4.4.14.6.1. 32 vCPU 2.1GHz
4.4.14.6.2. 128 GB RAM

4.4.15. ARMAZENAMENTO

4.4.15.1. O armazenamento disponível para as maquinas virtuais deverá considerar o armazenamento dos dados de forma persistente.
4.4.15.2. Permitir o gerenciamento de discos virtuais pela CONTRANTANTE através do portal WEB, desde sua criação, exclusão, expansão e anexo as máquinas virtuais no ambiente (VPC).
4.4.15.3. O(s) volume(s) criado(s) anexado(s) às máquinas virtuais deverão ser reconhecidos(s) pelo sistema operacional como um dispositivo físico local.
4.4.15.4. A solução de armazenamento deverá permitir que a CONTRATANTE defina a política de uso dos discos virtuais das máquinas virtuais em seu ambiente (VPC).
4.4.15.5. O armazenamento disponível e não alocado deverá permitir as seguintes características.
4.4.15.5.1. Expansão dos discos existentes das máquinas virtuais no ambiente (VPC)
4.4.15.5.2. Inclusão de novos discos nas máquinas virtuais existentes no ambiente (VPC)
4.4.15.5.3. Criação de novas máquinas virtuais no ambiente (VPC)
4.4.15.6. O armazenamento disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:
4.4.15.6.1. ALTA PERFORMANCE (SSD) 10 TB
4.4.15.6.2. BAIXA PERFORMANCE (HDD) 20 TB
4.4.15.7. OBJECT STORAGE 5 TB
4.4.15.7.1. Gerenciamento de quotas e permissões de acesso via interface WEB;
4.4.15.7.2. Compatível com API S3;
4.4.15.7.3. Os dados deverão estar localizados em território nacional;
4.4.15.7.4. O tráfego de dados (Download e Upload) deve ser ilimitado;
4.4.15.7.5. Os dados deverão estar acessíveis imediatamente sem restrições de acesso;

4.4.16. CONECTIVIDADE

4.4.16.1. Link Ponto a Ponto
4.4.16.1.1. A CONTRATADA deverá prover um link de dados ponto a ponto em fibra óptica

garantindo a banda dedicada para upload e download entre o site da CONTRATANTE e o datacenter da CONTRATADA onde se encontram os equipamentos que compõem a solução de datacenter virtual. Este link será utilizado exclusivamente para os serviços de comunicação entre datacenters;
4.4.16.1.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.
4.4.16.2. IP's públicos
4.4.16.2.1. A CONTRATADA deverá disponibilizar endereços IP fixos e públicos (válidos) para uso da CONTRATANTE de tal forma que lhe convir para uso em seu ambiente de produção.
4.4.16.3. Link de Internet VPC
4.4.16.3.1. A CONTRATADA deverá prover na VPC (Virtual Private Cloud) um link de internet dedicado de 100 Mbps para uso e comunicação das instâncias virtuais para a internet.
4.4.16.3.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

4.4.17. SOLUÇÃO DE PROTEÇÃO DOS DADOS

4.4.17.1. Deverá ser fornecido solução de segurança com as seguintes características mínimas para proteção do ambiente de contingencia e quarentena:
4.4.17.2. A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada;
4.4.17.3. A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo, 0.9 Gbps com as seguintes funcionalidades habilitadas simultaneamente: Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti-Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;
4.4.17.4. Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;
4.4.17.5. Deverá suportar e incluir licenciamento para, no mínimo, 2.000 Túneis VPN Lan-to-Lan (ou Gateway-to-Gateway) com VPN IPSec;
4.4.17.6. Deverá suportar e incluir licenciamento para, no mínimo, 32.000 usuários remotos (ou client-to-site) com VPN IPSec;
4.4.17.7. Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site) com VPN SSL;
4.4.17.8. Suporte a, no mínimo, 3.300.000 (três milhões e trezentos mil) conexões TCP simultâneas;
4.4.17.9. Suporte a, no mínimo, 140.000 (cento e quarenta mil) novas conexões TCP por segundo;
4.4.17.10. A solução deve possuir o licenciamento para, no mínimo, 10 sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 5 sistemas;
4.4.17.11. A solução deve possuir, no mínimo, 2 (duas) interfaces no padrão 10 GbE;
4.4.17.12. A solução deve possuir, no mínimo, 8 (oito) interfaces no padrão 1GbE;
4.4.17.13. CARACTERISTICAS
4.4.17.14. A solução deve possuir console para configuração e gerenciamento por interface de linha de comando (CLI);
4.4.17.15. Todas as portas de comunicação e interfaces devem ser capazes de funcionar simultaneamente oferecendo, cada uma, a plenitude de suas capacidades;
4.4.17.16. A solução deve apresentar armazenamento do tipo SSD (Solid-State Drive), com no mínimo 480GB;
4.4.17.17. A solução deve consistir em plataforma para centralização do gerenciamento, dos logs e geração de relatórios dos equipamentos que compõem a solução de segurança rede (NGFW);

4.4.17.18. A solução de gerenciamento, logs e relatoria deve ser do mesmo fabricante da solução de segurança de rede (NGFW);
4.4.17.19. As funcionalidades de centralização do gerenciamento, dos logs e geração de relatórios que compõe a plataforma, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;
4.4.17.20. Funcionalidades gerais para cluster de equipamentos
4.4.17.21. Funcionalidades gerais para Solução de Segurança de Perímetro (NGFW)
4.4.17.22. Funcionalidades Gerais e Recursos mínimos:
4.4.17.23. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
4.4.17.24. Deve suportar o protocolo padrão da indústria VXLAN;
4.4.17.25. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3 ad e LACP;
4.4.17.26. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing (PBR) ou policy based forwarding (PBF);
4.4.17.27. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
4.4.17.28. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
4.4.17.29. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
4.4.17.30. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
4.4.17.31. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
4.4.17.32. Deve suportar NAT dinâmico (Many-to-1);
4.4.17.33. Deve suportar NAT dinâmico (Many-to-Many);
4.4.17.34. Deve suportar NAT estático (1-to-1);
4.4.17.35. Deve suportar NAT estático (Many-to-Many);
4.4.17.36. Deve suportar NAT estático bidirecional 1-to-1;
4.4.17.37. Deve suportar Tradução de porta (PAT);
4.4.17.38. Deve suportar NAT de Origem;
4.4.17.39. Deve suportar NAT de Destino;
4.4.17.40. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
4.4.17.41. Deve poder combinar NAT de origem e NAT de destino na mesma politica
4.4.17.42. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.4.17.43. Deve suportar NAT64 e NAT46;
4.4.17.44. Deve implementar Equal-cost Multipath ECMP.
4.4.17.45. Deve suportar nativamente ou integração com soluções de SD-WAN;
4.4.17.46. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
4.4.17.47. Deve suportar o padrão do protocolo 'syslog' para geração e armazenamento dos logs usando o formato Common Event Format (CEF);
4.4.17.48. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);
4.4.17.49. Enviar log para sistemas de monitoração externos, simultaneamente;
4.4.17.50. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
4.4.17.51. Implementar Proteção anti-spoofing;
4.4.17.52. Deve identificar e bloquear comunicação com redes botnets;
4.4.17.53. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.
4.4.17.54. Deve possuir integração com LDAP para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos

equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

4.4.17.55. Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

4.4.17.56. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

4.4.17.57. Deve possuir funcionalidade de Single Sign-On. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

4.4.17.58. Deve possuir funcionalidade de Captive Portal local para autenticação de usuários que solicitem navegação através de políticas de firewall que façam o controle por usuários/grupos de usuários. Deve permitir também a customização deste Portal.

4.4.17.59. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.4.17.60. Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

4.4.17.61. Deve prover nativamente, no mínimo, licenciamento de uso de um (1) token, possibilitando autenticação de duplo fator para usuário administrador, acesso VPN e etc;

4.4.17.62. Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF);

4.4.17.63. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF e BGP);

4.4.17.64. Suportar OSPF graceful restart;

4.4.17.65. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

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

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

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

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

4.4.17.70. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

4.4.17.71. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

4.4.17.72. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

4.4.17.73. A configuração em alta disponibilidade deve sincronizar: Sessões;

4.4.17.74. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

4.4.17.75. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

4.4.17.76. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

4.4.17.77. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

4.4.17.78. Deve possuir suporte a criação de sistemas virtuais lógicos (contexto) no mesmo appliance;

4.4.17.79. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

4.4.17.80. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

4.4.17.81. Controle, inspeção e decriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
4.4.17.82. Deverá suportar controles por zona de segurança;
4.4.17.83. Controles de políticas por porta e protocolo;
4.4.17.84. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4.4.17.85. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
4.4.17.86. Firewall deve ser capaz de aplicar a inspeção de camada 7 (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
4.4.17.87. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
4.4.17.88. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4.4.17.89. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.4.17.90. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.4.17.91. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
4.4.17.92. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;
4.4.17.93. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.4.17.94. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
4.4.17.95. O gerenciamento da solução deve suportar acesso via interface WEB (HTTPS) e interface de linha de comando (SSH), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais lógicos por ambas interfaces;
4.4.17.96. Controle de Aplicações
4.4.17.97. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
4.4.17.98. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
4.4.17.99. Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.4.17.100. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4.4.17.101. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
4.4.17.102. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
4.4.17.103. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
4.4.17.104. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a

leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
4.4.17.105. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
4.4.17.106. Identificar o uso de táticas evasivas via comunicações criptografadas;
4.4.17.107. Atualizar a base de assinaturas de aplicações automaticamente;
4.4.17.108. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
4.4.17.109. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
4.4.17.110. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
4.4.17.111. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
4.4.17.112. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.4.17.113. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
4.4.17.114. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
4.4.17.115. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
4.4.17.116. Deve alertar o usuário quando uma aplicação for bloqueada;
4.4.17.117. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.118. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.119. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
4.4.17.120. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.121. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
4.4.17.122. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
4.4.17.123. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
4.4.17.124. Prevenção de Ameaças
4.4.17.125. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
4.4.17.126. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4.4.17.127. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

4.4.17.128. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
4.4.17.129. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
4.4.17.130. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
4.4.17.131. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.4.17.132. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
4.4.17.133. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
4.4.17.134. Deve permitir o bloqueio de vulnerabilidades;
4.4.17.135. Deve permitir o bloqueio de exploits conhecidos;
4.4.17.136. Deve incluir proteção contra-ataques de negação de serviços;
4.4.17.137. Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.4.17.138. Análise de padrões de estado de conexões;
4.4.17.139. Análise de decodificação de protocolo;
4.4.17.140. Análise para detecção de anomalias de protocolo;
4.4.17.141. Análise heurística;
4.4.17.142. IP Defragmentation;
4.4.17.143. Remontagem de pacotes de TCP;
4.4.17.144. Bloqueio de pacotes malformados;
4.4.17.145. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood;
4.4.17.146. Detectar e bloquear a origem de portscans;
4.4.17.147. Bloquear ataques efetuados por worms conhecidos;
4.4.17.148. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
4.4.17.149. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.4.17.150. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica;
4.4.17.151. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.4.17.152. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.4.17.153. Identificar e bloquear comunicação com botnets;
4.4.17.154. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
4.4.17.155. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
4.4.17.156. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
4.4.17.157. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
4.4.17.158. Os eventos devem identificar o país de onde partiu a ameaça;
4.4.17.159. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
4.4.17.160. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
4.4.17.161. Deve ser possível a configuração de diferentes políticas de controle de ameaças e

ataques baseada em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
4.4.17.162. Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise ou nuvem);
4.4.17.163. Filtro de URL
4.4.17.164. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.4.17.165. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.4.17.166. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
4.4.17.167. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4.4.17.168. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
4.4.17.169. Possuir pelo menos 50 categorias de URLs;
4.4.17.170. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
4.4.17.171. Permitir a customização de página de bloqueio;
4.4.17.172. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
4.4.17.173. Além do Explicit Web Proxy, suportar proxy Web transparente;
4.4.17.174. QoS e Traffic Shaping
4.4.17.175. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
4.4.17.176. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
4.4.17.177. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4.4.17.178. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
4.4.17.179. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;
4.4.17.180. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
4.4.17.181. Possibilitar a definição de tráfego com banda garantida;
4.4.17.182. Possibilitar a definição de tráfego com banda máxima;
4.4.17.183. Possibilitar a definição de fila de prioridade;
4.4.17.184. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
4.4.17.185. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
4.4.17.186. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
4.4.17.187. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
4.4.17.188. VPN
4.4.17.189. Suportar VPN Site-to-Site e Cliente-To-Site;
4.4.17.190. Suportar IPSec VPN e VPN SSL de forma simultânea;
4.4.17.191. A VPN IPSEC deve suportar 3DES;
4.4.17.192. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
4.4.17.193. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
4.4.17.194. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
4.4.17.195. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

4.4.17.196. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
4.4.17.197. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
4.4.17.198. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.4.17.199. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.4.17.200. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
4.4.17.201. Atribuição de DNS nos clientes remotos de VPN;
4.4.17.202. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
4.4.17.203. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
4.4.17.204. Suportar leitura e verificação de CRL (certificate revocation list);
4.4.17.205. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
4.4.17.206. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas:
4.4.17.207. Antes do usuário autenticar na estação;
4.4.17.208. Após autenticação do usuário na estação;
4.4.17.209. Sob demanda do usuário;
4.4.17.210. Deverá manter uma conexão segura com o portal durante a sessão;
4.4.17.211. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

4.4.18. SOLUÇÃO DE BACKUP

4.4.18.1. A Contratada deverá disponibilizar serviços que permitam realizar backup e restore rápidos dos servidores virtuais com retenção em storage.
4.4.18.2. A solução deverá ser licenciada por máquina virtual hospedada no ambiente Cloud Computing de contigencia;
4.4.18.3. As políticas de backup deverão ser configuradas conforme necessidades de tempo de retenção e periodicidade que o cliente desejar.
4.4.18.4. A fim de manter a integridade das informações e dos dados armazenados, a solução de Cloud Computing deverá garantir o backup das instâncias baseado nas características técnicas mínimas de uma solução de Backup conforme listadas abaixo:
4.4.18.5. Os Backup's poderão ser completos do tipo imagem dos volumes, sendo executados de forma automática (agendada) ou através de comandos manuais. Os backups das bases de dados de aplicações de execução contínua deverão ser realizados sem interrupção dos serviços (backup on line), e deverá ser utilizada uma rede de alta velocidade evitando que o tráfego de backup afete a operação normal dos sistemas.
4.4.18.6. Para realização da funcionalidade Backup e Restore, a Contratada deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de Backup deverá estar preparada para geração automática de imagens das máquinas virtuais /Snapshots, gravados em ambiente de armazenamento em nuvem da Contratada, que devem ser acessíveis aos recursos de Computação em Nuvem disponibilizados para a CONTRATANTE.
4.4.18.7. As políticas de backup poderão ser ajustadas para uma maior quantidade de backups diários e/ou retenção no repositório de armazenamento a ser disponibilizado para as cópias de segurança das instâncias contratadas respeitando a capacidade máxima contratada sem considerar eventuais ganhos com compressão e de duplicação.
4.4.18.8. Não serão permitidas soluções de backup de dados baseados em cópias realizadas de forma manual, nem baseadas em scripts automatizados, devendo ser utilizado um software de uso específico e dedicado para backup.
4.4.18.9. Não serão permitidas soluções de backup de dados baseados em sistemas operacionais

gratuitos ou de código aberto.

4.4.18.10. A solução proposta deverá dispor de software profissional para gerência e execução de backup e restauração de dados em nuvem, com garantia de atualizações e expansões durante o período do contrato sem ônus financeiro para a CONTRATANTE.

4.4.18.11. Deverá ter a capacidade de testar a consistência do backup e replicação (Sistema Operacional, aplicação, máquina virtual), emitindo relatório de auditoria para garantir a capacidade de recuperação, sempre que solicitado.

4.4.18.12. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório Microsoft Active Directory, possam recuperar objetos individuais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

4.4.18.13. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

4.4.18.14. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).

4.4.18.15. Deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.

4.4.18.16. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.

4.4.18.17. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.

4.4.18.18. Deverá permitir criar uma cópia da máquina virtual de produção para criação de ambiente de homologação, testes ou desenvolvimento, em qualquer estado anterior, para a resolução de problemas, provas de procedimentos ou capacitação.

4.4.18.19. Deverá permitir a recuperação de mais de uma máquina virtual e pontos de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

4.4.18.20. O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup.

4.4.18.21. O software deverá permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação e backup, sem necessidade de suspender a utilização de aplicações pelos usuários nem a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup.

4.4.18.22. O sistema deve prover quantidade ilimitada de restaurações, conforme as solicitações da CONTRATANTE, durante a vigência deste Contrato.

4.4.18.23. O console central de administração dos backups das máquinas virtuais deve ser via WEB e acessível via navegador utilizando protocolos HTTPS integrado a solução de Console de gestão do ambiente Cloud Computing.

4.4.18.24. Solução de backup para caixas de correio do Office365, conforme características abaixo:

4.4.18.25. O painel de administração do backup e restore das caixas de correio poderá ser separado da administração dos backups das máquinas virtuais, porém deverá ser da mesma fabricante.

4.4.19. RECUPERAÇÃO DE DESASTRES

4.4.19.1. Deverá fornecer solução de recuperação de desastres, baseado em replicação automatizada entre os datacenters da CONTRATADA.
4.4.19.2. A solução deverá ser integrada a mesma solução de gerenciamento do ambiente de máquinas virtuais, não sendo permitido utilização de software externos.
4.4.19.3. Garantir a proteção e replicação automatizada de máquinas virtuais.
4.4.19.4. Permitir a criação de planos de recuperação personalizáveis.
4.4.19.5. Deverá possuir funcionalidade de testes de plano de recuperação sem impacto.
4.4.19.6. Permitir a recuperação orquestrada quando necessário.
4.4.19.7. Permitir a replicação e recuperação para outro ambiente de Cloud Computing.
4.4.19.8. Permitir a utilização do ambiente em nuvem como datacenter secundário ou como um ambiente de recuperação.
4.4.19.9. Fornecer o monitoramento e envio de alertas do estado de suas instâncias protegidas.
4.4.19.10. A solução deverá permitir a reconfiguração das interfaces de rede destino.
4.4.19.11. A solução deverá disponibilizar a réplica de armazenamento em um segundo datacenter isolado do armazenamento de origem.
4.4.19.12. O armazenamento disponível para as maquinas virtuais replicadas deverão considerar o armazenamento dos dados de forma persistente.
4.4.19.13. O armazenamento da réplica disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:
4.4.19.13.1. ALTA PERFORMANCE (SSD)
4.4.19.13.2. BAIXA PERFORMANCE (HDD)
4.4.19.14. Solução de Desastre Padrão
4.4.19.14.1. A solução de desastres padrão deverá ser licenciada por máquina virtual.
4.4.19.14.2. A solução de desastre padrão deverá ser entregue com uma política de replicação a cada 24 horas.
4.4.19.15. Solução de Desastres Avançado
4.4.19.15.1. A solução de desastre avançada deverá ser licenciada por máquina virtual.
4.4.19.15.2. A solução de desastre avançada deverá ser entregue com uma política de replicação para no mínimo 15 minutos de RPO (Recovery Point Object).
4.4.19.15.3. A solução de desastre avançada deverá ser entregue com a funcionalidade de retenção para os pontos no tempo, provendo no mínimo 7 dias de retenção.

4.4.20. SOLUÇÃO DE DETECÇÃO E REPOSTA DE ENDPOINT
4.4.20.1. Requisitos gerais da solução:
4.4.20.1.1. Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.
4.4.20.1.2. Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento
4.4.20.1.3. A Solução de gerência deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.
4.4.20.1.4. A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.
4.4.20.1.5. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).
4.4.20.1.6. Deverá ser considerado o licenciamento para 25 dispositivos pelo período do contrato.
4.4.20.2. Requisitos e funcionalidades técnicos da solução:
4.4.20.2.1. A solução de proteção deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zeroday), ataques file-less, ameaças persistentes avançadas (APTs), ransomwares, exploits e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas.

4.4.20.2.2. A solução de proteção deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares com capacidade de restauração dos arquivos comprometidos.
4.4.20.2.3. A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.
4.4.20.2.4. A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.
4.4.20.2.5. Efetuar a análise baseada em técnicas de machine learning, inteligência artificial e threat intelligence, permitindo a proteção contra ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção.
4.4.20.2.6. Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITRE ATT&CK.
4.4.20.2.7. A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.
4.4.20.2.8. Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.
4.4.20.2.9. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.
4.4.20.2.10. Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:
4.4.20.2.11. Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);
4.4.20.2.12. Executar elevações de privilégio inesperadas;
4.4.20.2.13. Tentar se passar por processos do Windows;
4.4.20.2.14. Estabelecer conexões de rede suspeitas (call back ou command & control);
4.4.20.2.15. Uso suspeito do PSEXEC;
4.4.20.2.16. Invocação maliciosa através do Rundll;
4.4.20.2.17. Exploração ou modificação do arquivo hosts;
4.4.20.2.18. Tentativa de invocação de Remote Shell.
4.4.20.2.19. Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.
4.4.20.2.20. Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.
4.4.20.2.21. Bloquear exploits e payloads suspeitos do Metasploit.
4.4.20.2.22. As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.
4.4.20.2.23. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.
4.4.20.2.24. O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.
4.4.20.2.25. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.
4.4.20.2.26. Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.
4.4.20.2.27. Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:
4.4.20.2.28. Ignorar;
4.4.20.2.29. Registrar em log;
4.4.20.2.30. Alertar;
4.4.20.2.31. Bloquear;
4.4.20.2.32. Remover ou quarentenar;
4.4.20.2.33. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se

comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.

4.4.20.2.34. I - O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

4.4.20.2.35. II - Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

4.4.20.2.36. A solução deve possuir funcionalidade de EDR e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação.

4.4.20.2.37. A console deve oferecer uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

4.4.20.2.38. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas /modificadas, conexões de rede realizadas, dentre outras. Deve ser possível gerar relatório dessas informações.

4.4.20.2.39. A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.

4.4.20.2.40. Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.

4.4.20.2.41. A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do CONTRATANTE ou possuir mecanismos que possibilitem essa remoção.

4.4.20.2.42. A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:

4.4.20.2.43. Reputação de Arquivos (Com ou sem acesso à internet no endpoint);

4.4.20.2.44. IPS de Próxima Geração;

4.4.20.2.45. Proteção de Navegadores;

4.4.20.2.46. Aprendizado de Máquinas;

4.4.20.2.47. Análise Comportamental;

4.4.20.2.48. Mitigação da Exploração de Memória;

4.4.20.2.49. Controle e isolamento de Aplicações;

4.4.20.2.50. Controle de Dispositivos;

4.4.20.2.51. Emulação para Malware;

4.4.20.2.52. Proteção ao ambiente de Active Directory;

4.4.20.2.53. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.

4.4.20.2.54. Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.

4.4.20.2.55. De forma opcional ou não obrigatória a solução poderá a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

4.4.20.2.56. Criação de entradas falsas de cache, como Cache de DNS afim de enganar um invasor e identificar ações maliciosas no ambiente;

4.4.20.2.57. Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;

4.4.20.2.58. Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;

4.4.20.2.59. Criação de compartilhamentos de rede falsos em desktops;

4.4.20.2.60. Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas;

4.4.20.2.61. Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;

4.4.20.2.62. De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir

os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:
4.4.20.2.63. SEHOP - Structured Exception Handler Overwrite Protection;
4.4.20.2.64. Heap Spray (Exploits que iniciam através do HEAP);
4.4.20.2.65. Java Exploit Protection;
4.4.20.2.66. De forma opcional ou não obrigatória, a solução poderá se capaz de:
4.4.20.2.67. A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.
4.4.20.2.68. A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;
4.4.20.2.69. A solução poderá proteger contra intrusões por processo, usuário e terminal;
4.4.20.2.70. A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;
4.4.20.2.71. A solução poderá ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;
4.4.20.2.72. A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;
4.4.20.2.73. Instalação dos agentes:
4.4.20.2.74. A solução deve ser compatível com as versões de Sistema Operacionais:
4.4.20.2.75. Para computadores de usuários finais (estações: desktop, workstation e notebooks):
4.4.20.2.76. I - Microsoft Windows 7 (32-64bit) e superior em todas as suas distribuições (home, starter, professional, ultimate e enterprise).
4.4.20.2.77. Para servidores de rede físicos ou virtuais:
4.4.20.2.78. I - Microsoft Windows Server 2012 (64bit) e superior.
4.4.20.2.79. II - Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux, Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).
4.4.20.2.80. IV - O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware.
4.4.20.2.81. O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede.
4.4.20.2.82. Deve ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.
4.4.20.2.83. A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.
4.4.20.2.84. Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.
4.4.20.2.85. Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.
4.4.20.2.86. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;
4.4.20.2.87. Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.
4.4.20.2.88. Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.
4.4.20.2.89. Console de Gerência:
4.4.20.2.90. A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.
4.4.20.2.91. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes

navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.
4.4.20.2.92. A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.
4.4.20.2.93. Permitir no mínimo 5(cinco) acessos simultâneos.
4.4.20.2.94. A console e os agentes da solução devem possuir interface em português ou inglês.
4.4.20.2.95. Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.
4.4.20.2.96. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.
4.4.20.2.97. Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.
4.4.20.2.98. A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.
4.4.20.2.99. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.
4.4.20.2.100. Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.
4.4.20.2.101. Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.
4.4.20.2.102. Deve ser possível efetuar o “drill down” das consultas realizadas afim de avaliação mais detalhada das ocorrências.
4.4.20.2.103. A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.
4.4.20.2.104. Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:
4.4.20.2.105. Eventos de ameaças;
4.4.20.2.106. Eventos de comportamentos suspeitos;
4.4.20.2.107. Malwares detectados e bloqueados;
4.4.20.2.108. Computadores infectados.
4.4.20.2.109. Deve ser possível exportar os relatórios para o formato CSV ou PDF.
4.4.20.2.110. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.
4.4.20.2.111. A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.
4.4.20.2.112. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:
4.4.20.2.113. Nome da máquina;
4.4.20.2.114. Endereço IP;
4.4.20.2.115. Versão do sistema operacional (incluindo a versão do Service Pack);
4.4.20.2.116. Versão do agente;
4.4.20.2.117. Política aplicada.
4.4.20.2.118. A partir do console de gerenciamento da solução, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint para que aquele determinado equipamento seja movido para uma área de quarentena.
4.4.20.2.119. Monitoramento Assistido:
4.4.20.2.120. Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do CONTRATANTE.
4.4.20.2.121. Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;
4.4.20.2.122. Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);

4.4.20.2.123. Este serviço deverá ser prestado por equipe própria da CONTRATADA ou pela fabricante da solução;
4.4.20.2.124. Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;
4.4.20.2.125. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
4.4.20.2.126. A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, está não deverá atingir períodos superiores a 4 horas consecutivas;
4.4.20.2.127. A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;
4.4.20.2.128. O serviço deverá atender os seguintes requisitos:
4.4.20.2.129. Monitorar ferramentas de segurança;
4.4.20.2.130. Monitorar o armazenamento dos logs de eventos e e incidentes de segurança;
4.4.20.2.131. Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;
4.4.20.2.132. Iniciar tratamento de incidentes em até 10 min;
4.4.20.2.133. Realizar triagem, classificação e categorização de eventos de segurança da informação;
4.4.20.2.134. Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;
4.4.20.2.135. Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;
4.4.20.2.136. Registrar, escalar e notificar incidentes de segurança da informação;
4.4.20.2.137. Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;
4.4.20.2.138. Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;
4.4.20.2.139. Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;
4.4.20.2.140. Registrar e documentar ações e procedimentos realizados;
4.4.20.2.141. Emitir relatório semanal estatístico das operações realizadas;
4.4.20.2.142. Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;
4.4.20.2.143. Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;
4.4.20.2.144. Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;
4.4.20.2.145. Apoiar na definição, documentação e manutenção da normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE , visando refletir as definições instituídas por esses serviços de monitoramento;
4.4.20.2.146. Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;
4.4.20.2.147. Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;
4.4.20.2.148. Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.

4.4.20.2.149. Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;
4.4.20.2.150. Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;
4.4.20.2.151. Gerar subsídios e recomendações para elaboração de conteúdo para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;
4.4.20.2.152. Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;
4.4.20.2.153. Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.
4.4.20.2.154. Instalação da solução e repasse de conhecimento
4.4.20.2.155. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do CONTRATANTE, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.
4.4.20.2.156. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.
4.4.20.2.157. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do CONTRATANTE e em até 60 (sessenta) dias corridos para as unidades nas demais localidades, contados a partir da assinatura da Ordem de Serviço, conforme item 6.1.1.
4.4.20.2.158. A instalação compreenderá:
4.4.20.2.159. Implantação de todos os componentes em sua última versão estável.
4.4.20.2.160. Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.
4.4.20.2.161. Configuração de dashboards, relatórios e alertas, de maneira coordenada com o CONTRATANTE.
4.4.20.2.162. Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do CONTRATANTE, inclusive nas unidades descentralizadas nos estados da federação.
4.4.20.2.163. Instrução da equipe técnica do CONTRATANTE para a integração da a solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).
4.4.20.2.164. Documentação da topologia da solução, relatório das atividades e configurações realizadas.
4.4.20.2.165. Apresentação da solução configurada e implantada.
4.4.20.2.166. Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupo de até 4 pessoas, oferecido por técnico certificado na solução.
4.4.20.2.167. No repasse de conhecimento deve ser utilizado material em português.
4.4.20.2.168. Não é necessário que o repasse seja feito para um grupo fechado do CONTRATANTE e o mesmo pode ser realizado de forma remota.
4.4.20.2.169. O repasse de conhecimento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.
4.4.20.2.170. As datas dos repasses de conhecimento devem ser previamente combinadas com o CONTRATANTE.
4.4.20.2.171. Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.
4.4.20.2.172. Caso o repasse de conhecimento seja ministrado presencialmente e fora de São

Paulo, deverão estar incluídas as despesas com passagens aéreas, hospedagem e traslado entre aeroporto, hotel e local de treinamento.
4.4.20.2.173. O CONTRATANTE se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária. Neste caso, eventuais despesas de locomoção e estadia serão ressarcidas ao CONTRATANTE pela Contratada.
4.4.20.2.174. Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a média das notas seja inferior a 80% a contratada deverá ministrar novo repasse.
4.4.20.2.175. A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o CONTRATANTE, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

4.4.21. OPERAÇÃO, SUPORTE E GERENCIAMENTO

4.4.21.1. A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.
4.4.21.2. É responsabilidade da CONTRATADA monitorar a solução 24 x 7 x 365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.
4.4.21.3. A CONTRATADA será responsável por operar e gerenciar as tarefas de backup de acordo com as solicitações realizadas pelo time da CONTRATANTE, devendo adicionar, alterar ou remover tarefas e rotinas de backup, de acordo com as solicitações.
4.4.21.4. A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup.
4.4.21.5. Em casos de falha, a CONTRATADA deverá notificar prontamente o time da CONTRATANTE, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.
4.4.21.6. A CONTRATANTE terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup sem qualquer custo adicional.
4.4.21.7. A CONTRATADA deverá enviar mensalmente relatório estatístico das rotinas de backup.
4.4.21.8. A CONTRATADA deverá fornecer suporte técnico na modalidade 8 x 5 (8 horas por dia e 5 dias por semana) em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados à solução, através de suporte telefônico, por e-mail e através de um sistema online de chamados.
4.4.21.9. Em casos de acionamento de desastre, restaurações de bancos ou que seja necessária a restauração baremetal de um ou mais servidores, a CONTRATADA deve disponibilizar time técnico devidamente qualificado e de forma presencial nas dependências da CONTRATADA para a realização ou acompanhamento das tarefas.
4.4.21.10. A equipe técnica deverá estar alocada em até no máximo 4 horas na CONTRATANTE, após a constatação efetiva do desastre.
4.4.21.11. Durante a execução deste serviço a CONTRATADA se obriga a manter profissional (ais) com todas as qualificações.

4.4.22. PROVISIONAMENTO DO AMBIENTE CLOUD COMPUTING

4.4.22.1. A CONTRATADA será responsável por criar os novos servidores no ambiente de Cloud Computing, com as versões do sistema operacional e dos softwares básicos especificados pela CONTRATANTE.
4.4.22.2. Será de responsabilidade da equipe técnica da CONTRATADA, com o apoio da equipe técnica da CONTRATANTE, a migração das aplicações para o novo ambiente, sendo que a CONTRATANTE disponibilizará os recursos necessários, tanto de equipamentos quanto humanos, para apoiar a migração das aplicações.
4.4.22.3. Será de responsabilidade da equipe técnica da CONTRATADA o acompanhamento e auxilio a instalação dos softwares básicos e a migração das aplicações da CONTRATANTE, durante a migração a CONTRATANTE disponibilizará o conhecimento da estrutura das aplicações

e dos softwares básicos necessários (programas, diretórios, arquivos de configuração e demais informações) para a CONTRATADA afim de otimizar os recursos.
4.4.22.4. Após a finalização da migração das aplicações para o ambiente Cloud Computing, a CONTRATANTE disponibilizará uma equipe técnica para fazer os testes de homologação das aplicações migradas afim de atestar a conclusão da migração, sendo que os serviços contratados somente serão considerados como entregues aceitos após a conclusão dos testes.

4.5. CONDIÇÕES GERAIS

4.5.1. Permitir que os técnicos designados pela contratada, tenham pleno acesso ao(s) equipamento(s) a fim de executar os serviços de manutenção, objeto deste contrato, na presença de pessoa autorizada pela contratante.
4.5.2. Cada uma das partes deverá designar um funcionário para intermediar o relacionamento contratual com vistas a fiscalizar, e controlar a execução dos Serviços e uso de peças de reposição.
4.5.3. A parte que substituir o funcionário por ela designado deverá comunicar o fato imediatamente à outra parte.

Requisitos de Capacitação

4.6. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

Requisitos Legais

4.7. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

Requisitos de Experiência Profissional

4.8. Por se tratar de serviço que requer de seu executor conhecimentos técnicos especializados em face do grau de complexidade envolvida, o licitante vencedor deverá comprovar, através de atestado (s), declaração(ões) ou certidão(ões) de capacidade técnica expedido(s) por pessoa jurídica, de direito público ou privado, que comprove a aptidão para comercialização e implementação de Firewall baseado em appliance, visando assegurar a CONTRATANTE atender efetivamente os serviços pretendidos e descritos neste Termo de Referência.

Requisitos de Formação da Equipe

4.9. Em virtude da grande complexidade técnica do ambiente em produção na Fundação Casa, por se tratar de um ambiente em produção com aplicações críticas, bem como a fim de garantir a competência técnica para prestar os serviços objeto desta contratação, a licitante deverá comprovar que possui em seu quadro de colaboradores no mínimo 2 (dois) profissionais técnicos certificados pelo fabricante Dell nas áreas de servidores, storage e redes (network), além de 1 (um) profissional técnico certificado pelo fabricante Fortinet nas áreas de firewall.

5. Papéis e responsabilidades

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

5.2. São obrigações do CONTRATADO

5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5.. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.9. fazer a transição contratual, quando for o caso;

6. Modelo de execução do contrato

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: 05 dias da emissão da ordem de serviço.

Local da prestação dos serviços

6.2. Os serviços serão prestados no seguinte endereço: Sede Administrativa - Rua Florêncio de Abreu, 848, 9º andar, Luz, São Paulo - SP, CEP: 01030-001, observando o horário de funcionamento da instituição.

Especificação da garantia do serviço

6.3. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 36 (trinta e seis) meses, contados a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Formas de transferência de conhecimento

6.4. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

6.5. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Manutenção de Sigilo e Normas de Segurança

6.6. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

7. Modelo de gestão do contrato

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

Fiscalização

7.9. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

7.10. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto estadual nº 68.220, de 2023, art. 17).

7.11. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133, de 2021, art. 117, § 1º e Decreto estadual nº 68.220, de 2023, art. 17, II).

7.12. O fiscal técnico realizará, em conformidade com cronograma físico-financeiro, as medições dos serviços executados e aprovará a planilha de medição emitida pelo Contratado (Decreto estadual nº 68.220, de 2023, art. 17, III).

7.13. O fiscal técnico adotará medidas preventivas de controle de contratos, manifestando-se quanto à necessidade de suspensão da execução do objeto (Decreto estadual nº 68.220, de 2023, art. 17, IV).

7.14. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso (Lei federal nº 14.133, de 2021, artigo 117, § 2º).

7.15. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato (Decreto estadual nº 68.220, de 2023, art. 17, II).

Fiscalização Administrativa

7.16. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, II e III).

7.17. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência (Decreto estadual nº 68.220, de 2023, art. 18, IV).

7.18. Sempre que solicitado pelo Contratante, o Contratado deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, com a indicação dos empregados que preencherem as referidas vagas, nos termos do parágrafo único do artigo 116 da Lei nº 14.133, de 2021.

Gestor do Contrato

7.19. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e extinção do contrato (Decreto estadual nº 68.220, de 2023, inciso I do art. 2º).

7.20. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais (Decreto estadual nº 68.220, de 2023, art. 16, IX).

7.21. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações (Decreto estadual nº 68.220, de 2023, art. 18, VII).

7.22. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto estadual nº 68.220, de 2023, art. 16, VIII).

7.23. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração (Decreto estadual nº 68.220, de 2023, art. 16, VII e parágrafo único).

7.24. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato

Critérios de medição e pagamento

7.25. A avaliação da execução do objeto observará o disposto nesta seção.

7.26. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.26.1. não produzir os resultados acordados;

7.26.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.26.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

Do recebimento

7.27. Os serviços serão recebidos provisoriamente, no prazo de 04 (quatro) dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

7.27.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.28. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

7.29. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

7.30. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.31. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.31.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.32. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.33. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

7.34. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.35. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.36. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.37. Os serviços serão recebidos definitivamente no prazo de 04 (quatro) dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.37.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

7.37.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

7.37.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

7.37.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.37.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.38. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.39. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.40. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

7.41. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais (art. 7º, I, e §§ 2º e 3º, da Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, c/c o Decreto estadual nº 67.608, de 2023).

7.42. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.43. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.43.1. o prazo de validade;

7.43.2. a data da emissão;

7.43.3. os dados do contrato e do órgão contratante;

7.43.4. o período respectivo de execução do contrato;

7.43.5. o valor a pagar; e

7.43.6. eventual destaque do valor de retenções tributárias cabíveis.

7.44. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

7.45. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.46. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.47. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua

situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.48. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.49. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.50. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.51. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, inciso II, do Decreto estadual nº 67.608, de 2023.

7.52. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente na forma da legislação aplicável (art. 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o art. 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis, em relação ao atraso verificado.

Forma de pagamento

7.53. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do Contratado no Banco do Brasil S/A.

7.53.1. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do Contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo Contratado, de que os registros estão suspensos, nos termos do art. 8º da Lei estadual nº 12.799, de 2008.

7.54. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.55. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

7.55.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente

7.56. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. Do reajuste

8.1 Em conformidade com o inciso I do § 8º do art. 25 da Lei nº 14.133, de 2021, nas hipóteses de contratação de serviços contínuos sem regime de dedicação exclusiva de mão de obra e sem predominância de mão de obra, aplica-se a disciplina de reajustamento em sentido estrito, nos termos do inciso IV do art. 2º do Decreto estadual nº 67.608, de 2023, baseada no IPC-FIPE - Índice de Preços ao Consumidor elaborado pela Fundação Instituto de Pesquisas Econômicas da Universidade de São Paulo.

9. Critérios de seleção do fornecedor

Forma de seleção e critério de julgamento da proposta

9.1. *O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO e modo de disputa ABERTO.*

Regime de Execução

9.2. O regime de execução do contrato será de empreitada por preço global.

Da Aplicação da Margem de Preferência

9.3. Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

9.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos das seções subsequentes deste item 8, que serão exigidos conforme sua natureza jurídica:

Habilitação jurídica

9.5. **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.6. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

9.7. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.8. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

9.9. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.10. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

9.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

9.12. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

9.13. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.14. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.15. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.16. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.17. Prova de regularidade com a Fazenda Municipal/Distrital quanto ao Imposto sobre Serviços de Qualquer Natureza – ISSQN, do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.18. Caso o fornecedor se considere isento ou imune de tributos relacionados ao objeto contratual, em relação aos quais seja exigida regularidade fiscal neste instrumento, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.19. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

9.20. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de sociedade simples;

9.21. Certidão negativa de falência, expedida pelo distribuidor da sede do fornecedor, caso se trate de empresário individual ou sociedade empresária;

9.22. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um).

9.22.1. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei nº 14.133, de 2021, art. 65, § 1º).

9.22.2. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

9.22.3. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped, quando for o caso, ou outro limite estabelecido pela legislação aplicável.

9.23. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

9.24 Comprovação de capacidade para execução de serviço similar de complexidade tecnológica e operacional equivalente ou superior aos serviços a serem contratados, mediante a apresentação de de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso, que demonstrem, ao menos os seguintes elementos:

a) aptidão para comercialização e implementação de Firewall baseado em appliance;

b) deverá haver a comprovação da experiência mínima de 1 (um) ano na prestação de serviços similares, sendo aceito o somatório de atestados ou certidões de períodos diferentes, não havendo obrigatoriedade de os anos serem ininterruptos.

9.24.1. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do licitante;

9.24.2. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do (s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o objeto contratado, dentre outros documentos;

Outras comprovações

9.25. Declaração subscrita por representante legal do licitante, atestando que:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do art. 117, parágrafo único, da Constituição Estadual;

b) atenderá, na data da contratação, ao disposto no art. 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no art. 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso;

9.26. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que possui em seu quadro de colaboradores, no mínimo, 02 (dois) profissionais técnicos certificados pelo fabricante Dell nas áreas de servidores, storage e redes (network), além de 1 (um) profissional técnico certificado pelo fabricante Fortinet nas áreas de firewall.

9.27. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia e assistência técnica para os equipamentos listados no Anexo I.1 – parte A, deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

9.28. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware listados no Anexo I.1 – parte C serão prestados pelo próprio fabricante (Vmware e Fortinet), para todas as licenças existentes na Fundação CASA.

8.29. **Tratando-se de consórcio**:

8.29.1. Apresentação do compromisso público ou particular de constituição do consórcio, subscrito pelos consorciados, o qual deverá incluir, pelo menos, os seguintes elementos:

a) Designação do consórcio e sua composição;

b) Finalidade do consórcio;

c) Prazo de duração do consórcio, que deve coincidir, no mínimo, com o prazo de vigência contratual;

d) Endereço do consórcio e o foro competente para dirimir eventuais demandas entre os consorciados;

e) Definição das obrigações e responsabilidades de cada consorciado e das prestações específicas;

f) Previsão de responsabilidade solidária de todos os consorciados pelos atos praticados pelo consórcio, tanto na fase de licitação quanto na de execução do contrato, abrangendo também os encargos fiscais, trabalhistas e administrativos referentes ao objeto da contratação;

g) Indicação da empresa líder do consórcio e seu respectivo representante legal, que deverá ter poderes para receber citação, interpor e desistir de recursos, firmar a contratação e praticar todos os demais atos necessários à participação na licitação e execução do objeto contratado, sendo responsável pela representação do consórcio perante a Administração;

h) Compromisso subscrito pelas consorciadas de que o consórcio não terá a sua composição modificada sem a prévia e expressa anuência do Contratante até o integral cumprimento do objeto da contratação, observado o prazo de duração do consórcio, definido na alínea “c” deste subitem;

8.29.2. O licitante vencedor é obrigado a promover, antes da celebração da contratação, a constituição e o registro do consórcio, nos termos de seu compromisso de constituição.

8.29.3. Cada consorciado, individualmente, deverá atender as exigências relativas a habilitação jurídica e habilitação fiscal, social e trabalhista, e a certidão negativa de falência/insolvência. Para efeito de habilitação econômico-financeira e de habilitação técnica, quando exigida, será observado o disposto no inciso III do caput do art. 15 da Lei nº 14.133, de 2021;

8.29.4. Para efeito de habilitação econômico-financeira e de habilitação técnica, quando exigida, será observado o disposto no inciso III do caput do artigo 15 da Lei federal nº 14.133/2021.

8.29.5. A inabilitação de qualquer consorciado acarretará a automática inabilitação do consórcio.

8.30. **Tratando-se de cooperativas**, será exigida a seguinte documentação complementar, para evidenciar a observância do disposto no artigo 16 da Lei federal nº 14.133/2021:

8.30.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.30.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.30.3. Regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

8.30.4. Edital de convocação e ata da última assembleia geral, e registro de presença dos cooperados presentes nessa assembleia;

8.30.5. Ata da reunião em que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.30.6. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

8.30.7. Documentação que seja demonstrativa de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados, caso essa circunstância não esteja evidenciada na documentação a ser apresentada para atendimento aos subitens anteriores.

10. Estimativas do valor da contratação

[Conteúdo Sigiloso | Justificativa: 9.1 O art. 24 da Lei nº 14.133/2021 concede a discricionariedade para a Administração Pública, desde que justificado, a opção de adotar o caráter sigiloso do orçamento estimado da contratação, sem prejuízo do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas. Não prevalecendo, para tanto os órgãos de controle interno e externo. 9.2 Com fundamento no referido artigo, opta-se pela adoção do caráter sigiloso do orçamento destinado para a contratação, uma vez que tal modalidade possibilita maior atendimento aos princípios que regem a Administração Pública, como o da competividade, eficiência e da economicidade, conforme artigo 5º da lei ora mencionada. 9.3 O orçamento estimado com caráter sigiloso gera vantagem econômica no objeto da contratação a ser realizada, uma vez que o preço máximo estimado no procedimento não servirá como parâmetro para os participantes do procedimento licitatório, o que pode gerar economia para o ente público, bem como avaliará a participação de empresas com expertise e capacidade gerencial, inibindo, no futuro, eventual prejuízo na execução contratual. 9.4 O valor referencial obtido, em pesquisa de preços, para esta aquisição/serviço está muito superior ao praticado, atualmente, por esta Administração. Desta forma, o custo estimado da contratação possuirá caráter sigiloso e será tornado público em momento posterior à homologação.]

11. Adequação orçamentária

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Estado.

11.2. No presente exercício, a contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: Gestão/Unidade: SEC. DA JUSTIÇA E CIDADANIA / FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO - 990202;

II) Fonte de Recursos: 1.500.1.0.001;

III) Programa de Trabalho: 04.122.1729.6551.0000;

IV) Elemento de Despesa: 3.3.90.40.90.

11.3. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

12. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

VANESSA VALENTE

Autoridade competente

Assinou eletronicamente em 20/05/2025 às 18:56:33.

Termo de Referência 60/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
60/2025	990202-ESP-FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO	DENISE VITIRITO DE OLIVEIRA	20/05/2025 18:56 (v 9.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
I - alienação e concessão de direito real de uso de bens/Alienação		161.00039823/2025-01

1. Condições gerais da contratação

1.1. Contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	QTD	UNIDADE DE MEDIDA	ESPECIFICAÇÃO	CATSER	CÓD. SIAFISICO
1	1	Unidade	Serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter.	27090	39187

1.1.1. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.1.2. Este Termo de Referência foi elaborado em conformidade com o Decreto estadual nº 68.185, de 11 de dezembro de 2023.

1.1.3. O objeto desta contratação não se enquadra como serviços de luxo, observando o disposto no Decreto estadual nº 67.985, de 27 de setembro de 2023.

1.1.4. Considerando o valor estimado para a contratação, a presente licitação será de participação ampla, sendo aplicáveis as regras de tratamento favorecido constantes dos arts. 42 a 45 da Lei Complementar nº 123, de 2006, observado o disposto no § 2º do art. 4º da Lei nº 14.133, de 2021.

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar, elaborado nos termos do Decreto estadual nº 68.017, de 11 de outubro de 2023.

1.3. O(s) serviço(s) objeto desta contratação é enquadrado como contínuo, sem regime de dedicação exclusiva de mão de obra e sem predominância de mão de obra, tendo em vista a natureza da prestação em questão.

1.4. O prazo de vigência da contratação é de 12 (doze) meses, contados da data estabelecida para início dos serviços, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

Subcontratação

1.5. O Contratado não poderá subcontratar, ceder ou transferir, total ou parcialmente, o objeto contratual.

Validade da proposta

1.6. Para garantir a estabilidade da proposta e permitir a análise adequada do processo, especialmente em licitações mais complexas, a validade não será inferior a 180 (cento e oitenta) dias, a contar da data de sua apresentação.

1.6.1. Ressaltamos que esse prazo não traz custos extras aos fornecedores, uma vez que define um período razoável para a validade da proposta, seguindo as práticas do mercado, evitando retrabalho e assegurando a continuidade do certame sem prejuízos à Administração.

2. Descrição da solução

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3. Fundamentação e descrição da necessidade

3.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.3. O objeto da contratação está previsto no Plano de Contratações Anual 2024, que será executado em 2025, nos termos do Decreto Estadual nº 67.689, de 3 de maio de 2023, e segue divulgado no Portal Nacional de Contratações Públicas (PNPC) e no site institucional da Fundação Casa. A consulta ao PCA-2025 pode ser realizada através do link de acesso: https://fundacaocasa.sp.gov.br/index.php/plano-de-contratacao-anual/.

4. Requisitos da contratação

Requisitos de Negócio

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. Os itens a serem contratados serão licitados em apenas uma solução, prestados por uma única empresa visando a racionalização e gestão com ampla definição de responsabilidade em caso de acionamento da garantia, tendo em vista que todo o sistema tem grande complexidade, evitando-se comprometer a efetividade do serviço prestado.

4.1.2. Em virtude da complexidade do ambiente e da criticidade das aplicações existentes e em produção, os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte A, deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

4.1.3. Os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte B, poderão ser prestados diretamente pelo próprio fabricante correlacionado ao produto (Dell, IBM, HP, Fortinet, etc.) ou por seus parceiros autorizados.

4.1.4. Os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware e Fortigate listados na tabela – parte C, deverão ser prestados pelo próprio fabricante (Vmware e Fortinet) para todas as licenças existentes na Fundação Casa.

4.1.5. A fim de manter a qualidade dos serviços prestados para a Fundação Casa, caso haja a necessidade a CONTRATANTE poderá solicitar a substituição de qualquer equipamento listado na tabela, partes A e C, por um equipamento novo desde que se encontre em linha de produção e sem uso anterior devidamente aprovado pela equipe técnica da Fundação Casa. Este equipamento deverá ter performance igual ou superior ao já existente e deverá possuir garantia direta pelo fabricante do produto.

4.2. DA PRESTAÇÃO DO SERVIÇO

4.2.1. Visando conhecer o ambiente da CONTRATANTE, no início da vigência do contrato, em período a ser agendado, será realizada a etapa de OPERAÇÃO ASSISTIDA, na qual, durante no mínimo de 30 (trinta) dias, a CONTRATADA analisará e fornecerá, à CONTRATANTE, informações sobre a conformidade do ambiente (Configuração e Desempenho), no que tange a aplicação de atualização de SOFTWARE e HARDWARE.
4.2.2. O fornecimento das informações coletadas e analisadas deverá ocorrer em até 5 (cinco) dias após término da atividade de OPERAÇÃO ASSISTIDA.
4.2.3. A CONTRATADA se compromete a manter em correto e adequado funcionamento o “ambiente de processamento e armazenamento atual”, indicado no item 2, através da realização de SUPORTE TÉCNICO à CONTRATANTE.
4.2.4. A CONTRATADA atuará no “ambiente de processamento e armazenamento Dell”, tanto no HARDWARE quanto a SOFTWARE, realizando a aplicação de atualizações que vierem a ser disponibilizadas pelas fabricantes e a troca de itens que apresentem falha no decorrer do contrato.
4.2.5. O SUPORTE TÉCNICO ocorrerá em resposta à abertura de CHAMADO TÉCNICO realizada pela CONTRATANTE ou quando for detectada a necessidade de atuação no ambiente da CONTRATANTE, como, por exemplo, nos casos em que o fabricante disponibiliza um novo pacote de correção de erros.
4.2.6. A abertura de CHAMADO TÉCNICO pela CONTRATANTE será realizada por meio de ligação telefônica, envio de mensagem eletrônica ou registro em sistema próprio da CONTRATADA.
4.2.7. Cada CHAMADO TÉCNICO deverá receber identificação única e inequívoca.
4.2.8. Não deverá haver limitação quanto ao número de CHAMADOS TÉCNICOS que podem ser

abertos.

4.2.9. A existência de um CHAMADO TÉCNICO, independentemente da sua fase de atendimento, não deverá restringir a abertura de novos CHAMADOS TÉCNICOS.

4.2.10. A abertura de um novo CHAMADO TÉCNICO não implica no consequente encerramento de qualquer outro CHAMADO TÉCNICO.

4.2.11. A CONTRATADA deverá monitorar o envio de alertas pelos equipamentos do ambiente para, nos casos de envio de alerta, proceder à abertura de CHAMADO TÉCNICO.

4.2.12. Abertura de CHAMADO TÉCNICO e ATENDIMENTO TÉCNICO deverão estar disponíveis em regime 24x7 (24 horas por dia e 7 dias da semana).

4.2.13. As atividades de ATENDIMENTO TÉCNICO deverão ser realizadas por técnico da CONTRATADA e serão acompanhadas pela CONTRATANTE, devendo ser previamente agendadas.

4.2.14. Para os casos em que haja necessidade de interrupção dos serviços, mesmo que de forma parcial, o tempo total de indisponibilidade não deverá exceder 4 (quatro) horas.

4.2.15. Salvo manifestação contrária da CONTRATANTE, as atividades de atendimento técnico deverão ser realizadas presencialmente e fora do horário comercial.

4.2.16. A CONTRATADA deverá proceder ao atendimento dos CHAMADOS TÉCNICOS abertos observando os seguintes critérios:

4.2.17. Em até 2 horas da abertura, analista ou técnico da CONTRATADA deverá contatar a equipe da CONTRATANTE visando melhor entendimento do chamado, do estado do ambiente e, principalmente, para posicionar a equipe da CONTRATANTE sobre o procedimento que será executado pela CONTRATADA.

4.2.18. Em até 6 horas da abertura, para situações em que o ambiente esteja com o DESEMPENHO DEGRADADO ou em ESTADO CRÍTICO a CONTRATADA deverá proceder ao atendimento e conclusão do CHAMADO TÉCNICO, restaurando o ambiente ao seu modo normal de operação.

4.2.19. Para situações em que o ambiente não esteja em estado crítico ou com desempenho degradado a CONTRATADA disporá de 24 horas para atendimento e finalização do CHAMADO TÉCNICO.

4.2.20. A CONTRATADA deverá realizar visitas técnicas preventivas ao ambiente onde os equipamentos estão instalados. Estas visitas presenciais deverão ter periodicidade mínima mensal com duração mínima de 4 horas, podendo ser distribuídas entre as localidades, em dias úteis, de forma a verificar logs, mensagens de erros e eventuais atualizações de software ou correções preventivas.

4.2.21. A CONTRATADA deverá disponibilizar atendimento em língua portuguesa, sendo aceito para documentos que termos e textos técnicos poderão estar na língua inglesa.

4.2.22. Exceto para os casos de atualização e mudança de versão, quando detectada a necessidade de substituição de algum SOFTWARE a CONTRATADA deverá fornecer outro SOFTWARE que cumpra minimamente as funcionalidades daquele substituído.

4.2.23. O SOFTWARE, suas licenças e itens que este necessite deverão ser fornecidos objetivando o correto funcionamento e licenciamento do ambiente da CONTRATANTE.

4.2.24. A CONTRATADA deverá providenciar a renovação do suporte técnico oficial de todas as licenças de software de gerenciamento centralizado de virtualização do fabricante Vmware, conforme quantitativo do ANEXO I, listagem de softwares – Parte C, durante a vigência do contrato.

4.2.25. A CONTRATADA deverá providenciar a renovação do suporte técnico oficial e de todas as licenças de software de gerenciamento centralizado de virtualização do fabricante Fortigate, conforme quantitativo do ANEXO I, listagem de softwares – Parte C, durante a vigência do contrato.

4.2.26. Caso a CONTRATANTE identifique a necessidade de treinamento, devido a mudança do modo de operação do ambiente ou em decorrência da substituição, atualização ou upgrade de qualquer software utilizado pela CONTRATANTE, a CONTRATADA deverá providenciá-lo, em 2 turmas distintas, de modo a capacitar a equipe da CONTRATANTE a operar o novo SOFTWARE disponibilizado.

4.2.27. Detectada a necessidade de substituição de alguma PEÇA, esta deverá ser substituída

por uma peça nova, original e sem uso anterior.

4.2.28. Caso a substituição da PEÇA ocorra e haja necessidade de substituição de algum SOFTWARE, está substituição será de responsabilidade da CONTRATADA, devendo ser observadas e obedecidas as condições estabelecidas para os casos de substituição de SOFTWARE.

4.2.29. Sempre que for identificada a necessidade de substituição de algum item, independentemente deste representar uma PEÇA ou SOFTWARE, a CONTRATADA deverá obter a anuência formal do CONTRATANTE para a substituição pretendida.

4.2.30. A CONTRATANTE se reserva o direito de exigir a substituição dos equipamentos em definitivo por outro, com as mesmas características e capacidade, quando o mesmo apresentar repetidamente, máximo de 3 vezes, em 90 (noventa) dias, os mesmos defeitos durante a vigência do contrato. Caso a CONTRATANTE solicite a substituição de um determinado equipamento de hardware, o equipamento a ser entregue pela CONTRATADA deverá ser novo, sem uso anterior e com as especificações técnicas iguais ou superiores ao equipamento substituído.

4.2.31. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do Departamento de Tecnologia da Informação - DTI, referentes a qualquer problema detectado ou ao andamento de atividades de suporte técnico previstas.

4.2.32. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Fundação Casa ou a terceiros, por ocasião da prestação dos serviços, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente.

4.2.33. Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do(s) serviço(s) e o atendimento às especificações contidas no Contrato, Edital e em seus Anexos.

4.2.34. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato de Prestação de Serviço, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridas.

4.2.35. Substituir por outro profissional de qualificação igual ou superior qualquer um dos seus profissionais cuja qualificação, atuação, permanência ou comportamento decorrentes da execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina da repartição ou ao interesse do serviço público, sempre que exigido pelo Gestor do Contrato do Departamento de Tecnologia da Informação.

4.2.36. Comunicar, formal e imediatamente ao Gestor do Contrato, todas as ocorrências anormais e/ou que possam comprometer a execução dos serviços contratados.

4.2.37. Entregar mensalmente, para fins de controle, relatório de prestação de serviço de suporte técnico realizado no período. Deverão constar, no mínimo, as seguintes informações:

4.2.38. Relação de todos os chamados técnicos ocorridos no período, incluindo data e hora do início e término do atendimento.

4.2.39. Identificação do problema; severidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva

4.2.40. Data e hora do início e término da solução definitiva.

4.2.41. Identificação dos técnicos do Departamento Tecnologia Informação - DTI, que solicitou e validou o chamado.

4.2.42. Identificação do técnico do Fornecedor responsável pela execução do chamado, bem como outras informações pertinentes.

4.2.43. Prestar suporte técnico a todas as funcionalidades presentes e necessárias para o pleno estado de funcionamento dos equipamentos.

4.2.44. Manter sigilo sobre todo e qualquer assunto de interesse da Fundação CASA, ou de terceiros, de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

4.2.45. Responder pela reparação dos danos causados por defeitos relativos aos serviços prestados. Por isso deverá prezar pela qualidade e eficiência, garantindo que os serviços e também

as soluções definitivas fornecidas, não causem problemas adicionais àqueles apresentados pelo Departamento Tecnologia Informação – DTI, quando da abertura dos chamados técnicos.

4.2.46. A CONTRATANTE se reserva o direito de exigir da CONTRATADA, a seu único critério e a qualquer tempo durante a vigência do contrato, que alguns dos componentes considerados importantes, necessários e estratégicos para a execução deste contrato, como HD's, fontes e ventiladores, sejam armazenados no ambiente da CONTRATANTE durante a vigência do contrato, de forma a ser utilizada de maneira emergencial em caso de necessidade. Caso seja solicitada pela CONTRATANTE esse armazenamento local, as peças não utilizadas serão devolvidas à CONTRATADA ao término do contrato.

4.2.47. Deverão ser fornecidos, nas periodicidades abaixo indicadas, relatórios de acompanhamento com as seguintes características:

4.2.48. Reportar o número de CHAMADOS TÉCNICOS em aberto ou em atendimento, e CHAMADOS TÉCNICOS concluídos no mês anterior.

4.2.49. Descrição do motivo da abertura do CHAMADO TÉCNICO e descrição da solução, se concluído.

4.2.50. Periodicidade quadrimestral: Indicar as atualizações de hardware e software que necessitam ser aplicadas no ambiente.

4.2.51. A CONTRATADA deverá manter o sigilo de documentos e informações da CONTRATANTE a que eventualmente tenha acesso.

4.3. DO MONITORAMENTO DO AMBIENTE

4.3.1. A CONTRATADA deverá fornecer, implementar e suportar um serviço de monitoramento através de um centro de monitoramento de redes (NOC), capaz de monitorar os equipamentos do ambiente da CONTRATANTE, acompanhar alertas, , com no mínimo as seguintes características:

4.3.2. Solução de monitoramento utilizando dispositivo de hardware dedicado a função de monitoramento de infraestrutura, não sendo aceito soluções montadas sob a plataforma PC/x86 nem dispositivos montados usando soluções Open Source.

4.3.3. Deve permitir instalação em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

4.3.4. Deve possuir, no máximo, 1 RU (Rack Unit) de altura.

4.3.5. Deve possuir 2 fontes de alimentação AC bivolt interna, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).

4.3.6. Processador interno com quatro cores, Intel x86 ou equivalente, para permitir execução de aplicações internas tipo Dockers ou Kubernetes

4.3.7. Deve possuir 16 portas seriais com suporte a expansão até 96 portas seriais com conectores seriais RJ-45 em uma unidade "RU", sem a utilização de switches externos

4.3.8. Deve possuir para up-link ou aceso, no mínimo, 2 (duas) portas Gigabit Ethernet (10/100 /1000BT) com interface RJ-45 e 2 (duas) portas SFP+ 10GB.

4.3.9. Deve permitir alimentação de energia em corrente contínua (DC).

4.3.10. Deve possuir portas tipo USB para conectar modem celular, serial, ethernet, Wi-Fi, armazenamento e modem analógico e ou ethernet via conversor USB-Ethernet.

4.3.11. Deve permitir o acesso opcional via rede móvel LTE 5G/4G, devendo ser fornecido com chip de dados ativo;

4.3.12. Permitir acesso pelos protocolos HTTPS, SSHv2; opcional HTTP, Telnet and SSHv1.

4.3.13. Permitir a configuração via interface Gráfica ou linha de comando e Linux.

4.3.14. Deve suportar no mínimo 32GB de armazenamento interno.

4.3.15. Deve suportar as funções de servidor DHCP e executar roteamento e funções de firewall.

4.3.16. Deve suportar plataforma para Automação para end device via Python Scripts, Puppet, Chef, Docker e Ansible

4.3.17. Deve suportar automação via diferentes meios, incluindo, shell Script, Cloud, RESTFUL, ANSIBLE, Chef, Docker, KVM Hypervisor, Puppet, Python, RedHat Ansible, Ruby, Node.js JavaScript

4.3.18. Permitir Agrupamento de equipamentos via software em grupos associando múltiplas

unidades e permitir o gerenciamento através do login em uma das unidades apenas.
4.3.19. Envio de alertas e eventos deve permitir envio de mensagens via log de sistema, E-mail e na própria console.
4.3.20. Deve suportar a customização do nível de acesso de usuários.
4.3.21. Deve suportar a descoberta automática de novos dispositivos.
4.3.22. Deve permitir configurar suporte a NTP, zonas de horários mundiais ou sincronização através de torre de celular.
4.3.23. Deve permitir a restrição do acesso à interface de linha de comando (CLI) através de senha e dupla autenticação usando protocolos RSA e DUO.
4.3.24. Deve permite NAT e possuir funções de Firewall integrado com o sistema operacional. Deve suportar tunelamento através de SSL VPN, IPSec e Wireguard VPN.
4.3.25. Deve suportar mecanismos de AAA (Authentication, Authorization e Accounting), com suporte aos protocolos RADIUS e TACACS+, LDAP e Kerberos
4.3.26. Deve suportar o protoco IPv6;
4.3.27. Deve permitir a configuração de endereços IPv6 para gerenciamento;
4.3.28. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;
4.3.29. Deve suportar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH e HTTP sobre IPv6;
4.3.30. Deve suportar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6\ Suportar IPv4 / IPv6.

4.3.31. Solução para contingência e quarentena de arquivos potencionamente maliciosos;

4.3.32. O ambiente disponibilizado tem como finalidade testar e analisar arquivos potencialmente maliciosos em um ambiente seguro, controlado e isolado. Deverá permitir a execução de arquivos suspeitos, monitorando seu comportamento e suas interações com o sistema para detectar atividades maliciosas, como tentativas de explorar vulnerabilidades, modificações no sistema ou comunicação com servidores externos.
4.3.33. O ambiente deverá ser completamente isolado da rede corporativa e de sistemas de produção, prevenindo qualquer propagação de malware ou impactos negativos nos sistemas reais.
4.3.34. O ambiente deverá simular sistemas operacionais completos e redes de comunicação para capturar todas as ações realizadas pelo arquivo em teste.
4.3.35. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.

4.4. CARACTERISTICAS DA SOLUÇÃO DE CLOUD COMPUTING

4.4.1. Todos os equipamentos, software, infraestrutura e sustentação, necessários à implementação da solução proposta, são de inteira responsabilidade da Contratada, que deverá realizar de forma continuada tarefas e rotinas que garantam o pleno funcionamento de toda a infraestrutura, de forma integral e ininterrupta, ou seja, "24x7x365" (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) nas dependências da Contratada, mantendo em pleno funcionamento todo objeto da contratação.
4.4.2. Todos os equipamentos de hardware e software utilizados para a prestação de serviços devem ser de propriedade da licitante, que deverá ser responsável pela operação e manutenção dos equipamentos, não sendo permitida a revenda ou intermediação de serviços de terceiros.
4.4.3. A Contratada deverá gerenciar, monitorar, sustentar e operar de forma proativa todos os recursos disponibilizados para a CONTRATADA, de forma a garantir o correto funcionamento de todas as funcionalidades especificadas neste Termo de Referência, a partir de seu Centro de

Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana).

4.4.4. A solução de Computação em Nuvem ofertada deve permitir a criação de uma ou mais VPC´s (Virtual Private Cloud), de forma que a CONTRATADA possa provisionar uma seção da nuvem da solução ofertada isolada logicamente, onde é possível executar recursos da solução em uma rede virtual definida pela CONTRATADA, permitindo o controle total sobre seu ambiente de redes virtuais, incluindo a seleção do seu próprio intervalo de endereços IP, a criação de sub redes e a configuração de tabelas de rotas e gateways de rede, para acessar recursos e aplicações com segurança e facilidade. Além disso, a CONTRATADA poderá criar uma conexão de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e a VPC e aproveitar a nuvem da solução ofertada como uma extensão do seu datacenter corporativo.

4.4.5. A solução deverá ser escalável, de forma a permitir aumentar os recursos na infraestrutura de Cloud Computing da CONTRATADA para absorver a demanda complementar oriunda de picos de acesso ou expansão natural dos usuários em ambiente Cloud Computing.

4.4.6. Os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:

4.4.7. Implementar características de escalabilidade horizontal (novos servidores) e vertical (aumento de recursos do mesmo servidor), flexibilidade de configuração de memória, processador e disco.

4.4.8. Implementar a movimentação automática de servidores virtuais para redistribuição de carga e recuperação de falhas do ambiente físico.

4.4.9. É de responsabilidade da Contratada o monitoramento do hardware e seus componentes, bem como a manutenção dos mesmos, identificando necessidades de reposições, adaptações e melhorias, procedendo chamados aos fornecedores, acompanhando, garantindo a devida solução aos problemas que porventura ocorram, observando os tempos definidos no Nível de Serviço Exigido e fornecendo Console de Gestão para monitoramento em tempo real de todos os recursos computacionais.

4.4.10. O monitoramento deverá ser feito de forma continuada, não sobrecarregando os equipamentos ou consumindo recursos da solução de cloud computing provisionada aos clientes.

4.4.11. CARACTERISTICAS DA INFRAESTRUTURA FÍSICA

4.4.11.1. A solução proposta deverá hospedar os dados em datacenter localizado em território nacional;

4.4.11.2. Para fins de segurança da informação os dados deverão ser replicados entre datacenters com no mínimo 40km de distância entre eles. Em caso de desastre no datacenter principal o ambiente deverá estar disponível do datacenter réplica.

4.4.11.3. Os serviços de Cloud Computing a serem prestados deverão ser baseados em infraestrutura de Datacenter, que deverá manter compatibilidade com padrões internacionais, e deverão manter compatibilidade durante toda vigência do contrato.

4.4.11.4. As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviço atenderão, no mínimo, às características aqui definidas de estrutura física, instalações físicas, energia elétrica, climatização, proteção contra incêndio, segurança física, infraestrutura de acesso à internet do Datacenter e segurança lógica do Datacenter.

4.4.11.5. Os datacenters da CONTRATADA deverão possuir um ambiente com alta disponibilidade, atendendo aos seguintes requisitos mínimos:

4.4.11.5.1. Possuir certificação padrão TIER III;

4.4.11.5.2. Possuir no mínimo as seguintes certificações:

4.4.11.5.3. Garantir a disponibilidade imediata de energia elétrica através do fornecimento de sistemas de nobreaks independentes e redundantes

4.4.11.6. Redundância no fornecimento de portas de rede de acesso, através da disponibilidade de no mínimo dois switches distintos e independentes com portas Gigabit Ethernet ou superior com ao menos duas portas disponíveis em cada switch.

4.4.11.7. A fim de se comprovar o atendimento à estes requisitos mínimos, a CONTRATANTE se reserva o direito de realizar uma vistoria técnica presencial no ambiente da CONTRATADA, a

qualquer momento durante a vigência deste contrato, mediante agendamento prévio.
4.4.11.8. Caso ocorram quaisquer despesas de deslocamento ou viagem para a realização desta vistoria presencial, as despesas serão de responsabilidade da CONTRATADA.

4.4.12. CONSOLE DE GESTÃO DO AMBIENTE CLOUD COMPUTING

4.4.12.1. Permitir o gerenciamento da infraestrutura de Computação em Nuvem de forma independente de softwares de cliente (VNC, Remote Desktop, SSH, etc), por meio de API (Application Programming Interface), acessada via browser, de forma segura (HTTPS), utilizando-se de recursos de autenticação.
4.4.12.2. O acesso via interface web browser não poderá permitir a visualização ou edição de qualquer componente persistente a infraestrutura física que compõe a solução.
4.4.12.3. Possibilitar o cadastramento dos colaboradores da CONTRATANTE, inclusive, por perfil de acesso para administrar, operar ou consultar o ambiente de produção da solução na infraestrutura de Computação em Nuvem disponibilizada pela CONTRATADA.
4.4.12.4. Permitir selecionar modelos preexistentes (templates) de máquinas virtuais e sistemas operacionais.
4.4.12.5. Permitir personalizar modelos (templates) que melhor se adaptem às necessidades da CONTRATANTE.
4.4.12.6. Permitir modificar os recursos da Infraestrutura de Computação em Nuvem e atualizá-los de uma forma controlada e previsível, aplicando-se, quando necessário, controles de versionamento, devendo ser permitido o rastreamento das alterações históricas efetuadas no ambiente.
4.4.12.7. Disponibilizar console via interface gráfica afim de permitir o agendamento, realização de backups e horários de funcionamento por recurso (servidor; banco de dados, fileserver), por ambiente (produção) ou por etiqueta (classificação das soluções/sistemas).
4.4.12.8. Deverá ser disponibilizado um painel de controle (software de gestão para alojamento web) com as opções mínimas de: gerenciamento FTP, gerenciamento de arquivos, gerenciamento de banco de dados, verificação de estatísticas, gerenciamento de domínios;
4.4.12.9. Conexão a 2 pontos de troca de trafego distintos;
4.4.12.10. Deverá possuir gerenciador de arquivos web;
4.4.12.11. Deverá possuir painel de gerenciamento de DNS.

4.4.13. MONITORAMENTO DE RECURSOS

4.4.13.1. A Contratada deverá oferecer Console de Gestão de fácil utilização e que permita criar e gerenciar os recursos e/ou grupo de recursos relacionados ao serviço de Computação em Nuvem por meio de web browsers.
4.4.13.2. A solução ofertada deverá permitir o monitoramento das máquinas virtuais, provendo o monitoramento do ambiente de Computação em Nuvem (serviços e recursos), de forma automatizada e abrangendo servidores, sistemas operacionais e recursos de comunicação, em tempo real (24x7x365), visando detectar problemas (incidentes), no que tange à sustentação operacional e não a aplicação do Contratante.
4.4.13.3. Prover o monitoramento constante em amostras com granularidade mínima de 1 hora (24X7X365) dos serviços e recursos, visando detectar os problemas mais frequentes, informando a CONTRATANTE a ocorrência destes.
4.4.13.4. Deverá ser realizada pela Contratada a monitoração da qualidade e nível de utilização da infraestrutura de acesso à Internet, disponibilizada pela solução ofertada pela Contratada, bem como as resoluções em caso de problemas.
4.4.13.5. Deverá permitir a visualização dos indicadores de desempenho, falhas do ambiente e características e requisitos operacionais dos recursos gerenciados por meio do painel de apresentação (dashboard) Online (tempo real).
4.4.13.6. A solução ofertada deverá prover alarmes para a Console de Gestão de eventos,

mostrando quais recursos estiveram acima do threshold, permitindo gerar relatório a partir dos eventos observados.
4.4.13.7. Para cada servidor virtual, deverá ser possível o acompanhamento e monitoramento dos seguintes recursos: vCPU, RAM, Tráfego de Rede (In/Out) e Disco.

4.4.14. SERVIDORES VIRTUALIZADOS E RECURSOS COMPUTACIONAIS

4.4.14.1. Todos os servidores virtuais deverão ser disponibilizados em ambiente de Cloud Computing, em ambiente seguro e separados logicamente de outros clientes, com as seguintes funcionalidades:
4.4.14.2. Implementar características de escalabilidade vertical (aumento/diminuição de recursos do mesmo servidor), incluindo flexibilidade de configuração de memória, processador e disco;
4.4.14.3. Permitir a criação, pela CONTRATANTE, de pelo menos 1 (uma) imagem (snapshot) dos servidores virtuais sem custo adicional;
4.4.14.4. Assegurar a comunicação segura e encriptada entre os próprios servidores e os clientes que farão acesso aos mesmos, através de protocolo seguro HTTPS, ou seja, todos os servidores deverão ser disponibilizados com certificados digitais SSL instalados.
4.4.14.5. Os recursos computacionais adicionais, poderão ser utilizados para agregação ou distribuição entre os servidores virtualizados existentes ou para a criação de novos servidores virtuais;
4.4.14.6. Deverá ser considerado um pool de recursos computacionais para suprir a demanda de todas as máquinas virtuais do ambiente atualmente em produção e no mínimo com as seguintes características Processador e Memória.
4.4.14.6.1. 32 vCPU 2.1GHz
4.4.14.6.2. 128 GB RAM

4.4.15. ARMAZENAMENTO

4.4.15.1. O armazenamento disponível para as maquinas virtuais deverá considerar o armazenamento dos dados de forma persistente.
4.4.15.2. Permitir o gerenciamento de discos virtuais pela CONTRANTANTE através do portal WEB, desde sua criação, exclusão, expansão e anexo as máquinas virtuais no ambiente (VPC).
4.4.15.3. O(s) volume(s) criado(s) anexado(s) às máquinas virtuais deverão ser reconhecidos(s) pelo sistema operacional como um dispositivo físico local.
4.4.15.4. A solução de armazenamento deverá permitir que a CONTRATANTE defina a política de uso dos discos virtuais das máquinas virtuais em seu ambiente (VPC).
4.4.15.5. O armazenamento disponível e não alocado deverá permitir as seguintes características.
4.4.15.5.1. Expansão dos discos existentes das máquinas virtuais no ambiente (VPC)
4.4.15.5.2. Inclusão de novos discos nas máquinas virtuais existentes no ambiente (VPC)
4.4.15.5.3. Criação de novas máquinas virtuais no ambiente (VPC)
4.4.15.6. O armazenamento disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:
4.4.15.6.1. ALTA PERFORMANCE (SSD) 10 TB
4.4.15.6.2. BAIXA PERFORMANCE (HDD) 20 TB
4.4.15.7. OBJECT STORAGE 5 TB
4.4.15.7.1. Gerenciamento de quotas e permissões de acesso via interface WEB;
4.4.15.7.2. Compatível com API S3;
4.4.15.7.3. Os dados deverão estar localizados em território nacional;
4.4.15.7.4. O tráfego de dados (Download e Upload) deve ser ilimitado;
4.4.15.7.5. Os dados deverão estar acessíveis imediatamente sem restrições de acesso;

4.4.16. CONECTIVIDADE

4.4.16.1. Link Ponto a Ponto
4.4.16.1.1. A CONTRATADA deverá prover um link de dados ponto a ponto em fibra óptica

garantindo a banda dedicada para upload e download entre o site da CONTRATANTE e o datacenter da CONTRATADA onde se encontram os equipamentos que compõem a solução de datacenter virtual. Este link será utilizado exclusivamente para os serviços de comunicação entre datacenters;
4.4.16.1.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.
4.4.16.2. IP's públicos
4.4.16.2.1. A CONTRATADA deverá disponibilizar endereços IP fixos e públicos (válidos) para uso da CONTRATANTE de tal forma que lhe convir para uso em seu ambiente de produção.
4.4.16.3. Link de Internet VPC
4.4.16.3.1. A CONTRATADA deverá prover na VPC (Virtual Private Cloud) um link de internet dedicado de 100 Mbps para uso e comunicação das instâncias virtuais para a internet.
4.4.16.3.2. O volume de tráfego de dados ofertado deve ser ilimitado, tanto no sentido de download como upload, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

4.4.17. SOLUÇÃO DE PROTEÇÃO DOS DADOS

4.4.17.1. Deverá ser fornecido solução de segurança com as seguintes características mínimas para proteção do ambiente de contingencia e quarentena:
4.4.17.2. A solução deverá suportar throughput (Taxa de Transferência) de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada;
4.4.17.3. A solução deve suportar Throughput (Taxa de Transferência) de, no mínimo, 0.9 Gbps com as seguintes funcionalidades habilitadas simultaneamente: Firewall, Controle de Aplicação e Prevenção de Ameaças (Anti-Malware, IPS, Application Control URL Filtering). Esta taxa deve referenciar-se a tráfego multiprotocolo em ambiente de produção, tráfego considerado de mundo real ou tráfego misto, ou seja, aquele que não faz referência apenas a um protocolo e/ou um tamanho de pacote para teste em condição ideal;
4.4.17.4. Suportar throughput (Taxa de Transferência) de, no mínimo, 1 Gbps de VPN IPsec;
4.4.17.5. Deverá suportar e incluir licenciamento para, no mínimo, 2.000 Túneis VPN Lan-to-Lan (ou Gateway-to-Gateway) com VPN IPSec;
4.4.17.6. Deverá suportar e incluir licenciamento para, no mínimo, 32.000 usuários remotos (ou client-to-site) com VPN IPSec;
4.4.17.7. Deverá suportar e incluir licenciamento para, no mínimo, 500 usuários remotos (ou client-to-site) com VPN SSL;
4.4.17.8. Suporte a, no mínimo, 3.300.000 (três milhões e trezentos mil) conexões TCP simultâneas;
4.4.17.9. Suporte a, no mínimo, 140.000 (cento e quarenta mil) novas conexões TCP por segundo;
4.4.17.10. A solução deve possuir o licenciamento para, no mínimo, 10 sistemas virtuais lógicos (Contextos), independentes entre si e estar licenciado e/ou ter incluído sem custo adicional pelo menos 5 sistemas;
4.4.17.11. A solução deve possuir, no mínimo, 2 (duas) interfaces no padrão 10 GbE;
4.4.17.12. A solução deve possuir, no mínimo, 8 (oito) interfaces no padrão 1GbE;
4.4.17.13. CARACTERISTICAS
4.4.17.14. A solução deve possuir console para configuração e gerenciamento por interface de linha de comando (CLI);
4.4.17.15. Todas as portas de comunicação e interfaces devem ser capazes de funcionar simultaneamente oferecendo, cada uma, a plenitude de suas capacidades;
4.4.17.16. A solução deve apresentar armazenamento do tipo SSD (Solid-State Drive), com no mínimo 480GB;
4.4.17.17. A solução deve consistir em plataforma para centralização do gerenciamento, dos logs e geração de relatórios dos equipamentos que compõem a solução de segurança rede (NGFW);

4.4.17.18. A solução de gerenciamento, logs e relatoria deve ser do mesmo fabricante da solução de segurança de rede (NGFW);
4.4.17.19. As funcionalidades de centralização do gerenciamento, dos logs e geração de relatórios que compõe a plataforma, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;
4.4.17.20. Funcionalidades gerais para cluster de equipamentos
4.4.17.21. Funcionalidades gerais para Solução de Segurança de Perímetro (NGFW)
4.4.17.22. Funcionalidades Gerais e Recursos mínimos:
4.4.17.23. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
4.4.17.24. Deve suportar o protocolo padrão da indústria VXLAN;
4.4.17.25. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3 ad e LACP;
4.4.17.26. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing (PBR) ou policy based forwarding (PBF);
4.4.17.27. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
4.4.17.28. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
4.4.17.29. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
4.4.17.30. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
4.4.17.31. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
4.4.17.32. Deve suportar NAT dinâmico (Many-to-1);
4.4.17.33. Deve suportar NAT dinâmico (Many-to-Many);
4.4.17.34. Deve suportar NAT estático (1-to-1);
4.4.17.35. Deve suportar NAT estático (Many-to-Many);
4.4.17.36. Deve suportar NAT estático bidirecional 1-to-1;
4.4.17.37. Deve suportar Tradução de porta (PAT);
4.4.17.38. Deve suportar NAT de Origem;
4.4.17.39. Deve suportar NAT de Destino;
4.4.17.40. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
4.4.17.41. Deve poder combinar NAT de origem e NAT de destino na mesma politica
4.4.17.42. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
4.4.17.43. Deve suportar NAT64 e NAT46;
4.4.17.44. Deve implementar Equal-cost Multipath ECMP.
4.4.17.45. Deve suportar nativamente ou integração com soluções de SD-WAN;
4.4.17.46. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
4.4.17.47. Deve suportar o padrão do protocolo 'syslog' para geração e armazenamento dos logs usando o formato Common Event Format (CEF);
4.4.17.48. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);
4.4.17.49. Enviar log para sistemas de monitoração externos, simultaneamente;
4.4.17.50. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
4.4.17.51. Implementar Proteção anti-spoofing;
4.4.17.52. Deve identificar e bloquear comunicação com redes botnets;
4.4.17.53. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.
4.4.17.54. Deve possuir integração com LDAP para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos

equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

4.4.17.55. Deve possuir integração com Radius para identificação de usuários e grupos de usuários, permitindo que os mesmos sejam utilizados, ao menos, no acesso administrativo dos equipamentos, autenticação VPN e políticas de firewall, dando assim maior granularidade e controle.

4.4.17.56. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

4.4.17.57. Deve possuir funcionalidade de Single Sign-On. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

4.4.17.58. Deve possuir funcionalidade de Captive Portal local para autenticação de usuários que solicitem navegação através de políticas de firewall que façam o controle por usuários/grupos de usuários. Deve permitir também a customização deste Portal.

4.4.17.59. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.4.17.60. Deve permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;

4.4.17.61. Deve prover nativamente, no mínimo, licenciamento de uso de um (1) token, possibilitando autenticação de duplo fator para usuário administrador, acesso VPN e etc;

4.4.17.62. Para IPv4, deve suportar roteamento estático e dinâmico (RIP, BGP e OSPF);

4.4.17.63. Para IPv6, deve suportar roteamento estático e dinâmico (OSPF e BGP);

4.4.17.64. Suportar OSPF graceful restart;

4.4.17.65. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

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

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

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

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

4.4.17.70. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

4.4.17.71. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

4.4.17.72. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

4.4.17.73. A configuração em alta disponibilidade deve sincronizar: Sessões;

4.4.17.74. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

4.4.17.75. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

4.4.17.76. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

4.4.17.77. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

4.4.17.78. Deve possuir suporte a criação de sistemas virtuais lógicos (contexto) no mesmo appliance;

4.4.17.79. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;

4.4.17.80. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

4.4.17.81. Controle, inspeção e decriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
4.4.17.82. Deverá suportar controles por zona de segurança;
4.4.17.83. Controles de políticas por porta e protocolo;
4.4.17.84. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
4.4.17.85. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
4.4.17.86. Firewall deve ser capaz de aplicar a inspeção de camada 7 (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
4.4.17.87. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
4.4.17.88. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
4.4.17.89. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.4.17.90. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
4.4.17.91. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
4.4.17.92. Suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;
4.4.17.93. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
4.4.17.94. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
4.4.17.95. O gerenciamento da solução deve suportar acesso via interface WEB (HTTPS) e interface de linha de comando (SSH), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais lógicos por ambas interfaces;
4.4.17.96. Controle de Aplicações
4.4.17.97. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
4.4.17.98. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
4.4.17.99. Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
4.4.17.100. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
4.4.17.101. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
4.4.17.102. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
4.4.17.103. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
4.4.17.104. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a

leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
4.4.17.105. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
4.4.17.106. Identificar o uso de táticas evasivas via comunicações criptografadas;
4.4.17.107. Atualizar a base de assinaturas de aplicações automaticamente;
4.4.17.108. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
4.4.17.109. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
4.4.17.110. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
4.4.17.111. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
4.4.17.112. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.4.17.113. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
4.4.17.114. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
4.4.17.115. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
4.4.17.116. Deve alertar o usuário quando uma aplicação for bloqueada;
4.4.17.117. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.118. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.119. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
4.4.17.120. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
4.4.17.121. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
4.4.17.122. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
4.4.17.123. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
4.4.17.124. Prevenção de Ameaças
4.4.17.125. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
4.4.17.126. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
4.4.17.127. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

4.4.17.128. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
4.4.17.129. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
4.4.17.130. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
4.4.17.131. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.4.17.132. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
4.4.17.133. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
4.4.17.134. Deve permitir o bloqueio de vulnerabilidades;
4.4.17.135. Deve permitir o bloqueio de exploits conhecidos;
4.4.17.136. Deve incluir proteção contra-ataques de negação de serviços;
4.4.17.137. Deverá possuir os seguintes mecanismos de inspeção de IPS:
4.4.17.138. Análise de padrões de estado de conexões;
4.4.17.139. Análise de decodificação de protocolo;
4.4.17.140. Análise para detecção de anomalias de protocolo;
4.4.17.141. Análise heurística;
4.4.17.142. IP Defragmentation;
4.4.17.143. Remontagem de pacotes de TCP;
4.4.17.144. Bloqueio de pacotes malformados;
4.4.17.145. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood;
4.4.17.146. Detectar e bloquear a origem de portscans;
4.4.17.147. Bloquear ataques efetuados por worms conhecidos;
4.4.17.148. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
4.4.17.149. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.4.17.150. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica;
4.4.17.151. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.4.17.152. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.4.17.153. Identificar e bloquear comunicação com botnets;
4.4.17.154. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
4.4.17.155. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
4.4.17.156. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
4.4.17.157. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
4.4.17.158. Os eventos devem identificar o país de onde partiu a ameaça;
4.4.17.159. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
4.4.17.160. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
4.4.17.161. Deve ser possível a configuração de diferentes políticas de controle de ameaças e

ataques baseada em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
4.4.17.162. Fornecer proteção contra-ataques de dia zero por meio de estreita integração com os componentes Sandbox (on-premise ou nuvem);
4.4.17.163. Filtro de URL
4.4.17.164. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
4.4.17.165. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
4.4.17.166. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
4.4.17.167. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
4.4.17.168. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
4.4.17.169. Possuir pelo menos 50 categorias de URLs;
4.4.17.170. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
4.4.17.171. Permitir a customização de página de bloqueio;
4.4.17.172. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
4.4.17.173. Além do Explicit Web Proxy, suportar proxy Web transparente;
4.4.17.174. QoS e Traffic Shaping
4.4.17.175. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
4.4.17.176. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
4.4.17.177. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
4.4.17.178. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
4.4.17.179. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;
4.4.17.180. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
4.4.17.181. Possibilitar a definição de tráfego com banda garantida;
4.4.17.182. Possibilitar a definição de tráfego com banda máxima;
4.4.17.183. Possibilitar a definição de fila de prioridade;
4.4.17.184. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
4.4.17.185. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
4.4.17.186. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
4.4.17.187. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;
4.4.17.188. VPN
4.4.17.189. Suportar VPN Site-to-Site e Cliente-To-Site;
4.4.17.190. Suportar IPSec VPN e VPN SSL de forma simultânea;
4.4.17.191. A VPN IPSEC deve suportar 3DES;
4.4.17.192. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
4.4.17.193. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
4.4.17.194. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
4.4.17.195. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

4.4.17.196. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI;
4.4.17.197. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
4.4.17.198. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
4.4.17.199. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
4.4.17.200. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
4.4.17.201. Atribuição de DNS nos clientes remotos de VPN;
4.4.17.202. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
4.4.17.203. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
4.4.17.204. Suportar leitura e verificação de CRL (certificate revocation list);
4.4.17.205. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
4.4.17.206. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas:
4.4.17.207. Antes do usuário autenticar na estação;
4.4.17.208. Após autenticação do usuário na estação;
4.4.17.209. Sob demanda do usuário;
4.4.17.210. Deverá manter uma conexão segura com o portal durante a sessão;
4.4.17.211. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

4.4.18. SOLUÇÃO DE BACKUP

4.4.18.1. A Contratada deverá disponibilizar serviços que permitam realizar backup e restore rápidos dos servidores virtuais com retenção em storage.
4.4.18.2. A solução deverá ser licenciada por máquina virtual hospedada no ambiente Cloud Computing de contigencia;
4.4.18.3. As políticas de backup deverão ser configuradas conforme necessidades de tempo de retenção e periodicidade que o cliente desejar.
4.4.18.4. A fim de manter a integridade das informações e dos dados armazenados, a solução de Cloud Computing deverá garantir o backup das instâncias baseado nas características técnicas mínimas de uma solução de Backup conforme listadas abaixo:
4.4.18.5. Os Backup's poderão ser completos do tipo imagem dos volumes, sendo executados de forma automática (agendada) ou através de comandos manuais. Os backups das bases de dados de aplicações de execução contínua deverão ser realizados sem interrupção dos serviços (backup on line), e deverá ser utilizada uma rede de alta velocidade evitando que o tráfego de backup afete a operação normal dos sistemas.
4.4.18.6. Para realização da funcionalidade Backup e Restore, a Contratada deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de Backup deverá estar preparada para geração automática de imagens das máquinas virtuais /Snapshots, gravados em ambiente de armazenamento em nuvem da Contratada, que devem ser acessíveis aos recursos de Computação em Nuvem disponibilizados para a CONTRATANTE.
4.4.18.7. As políticas de backup poderão ser ajustadas para uma maior quantidade de backups diários e/ou retenção no repositório de armazenamento a ser disponibilizado para as cópias de segurança das instâncias contratadas respeitando a capacidade máxima contratada sem considerar eventuais ganhos com compressão e de duplicação.
4.4.18.8. Não serão permitidas soluções de backup de dados baseados em cópias realizadas de forma manual, nem baseadas em scripts automatizados, devendo ser utilizado um software de uso específico e dedicado para backup.
4.4.18.9. Não serão permitidas soluções de backup de dados baseados em sistemas operacionais

gratuitos ou de código aberto.

4.4.18.10. A solução proposta deverá dispor de software profissional para gerência e execução de backup e restauração de dados em nuvem, com garantia de atualizações e expansões durante o período do contrato sem ônus financeiro para a CONTRATANTE.

4.4.18.11. Deverá ter a capacidade de testar a consistência do backup e replicação (Sistema Operacional, aplicação, máquina virtual), emitindo relatório de auditoria para garantir a capacidade de recuperação, sempre que solicitado.

4.4.18.12. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de serviços de diretório Microsoft Active Directory, possam recuperar objetos individuais como usuários, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

4.4.18.13. Deverá incluir ferramentas de recuperação, mediante as quais os administradores dos servidores de banco de dados Microsoft SQL Server, possam recuperar objetos individuais, tais como bases, tabelas, registros, entre outros, sem a necessidade de recuperar os arquivos das máquinas virtuais como um todo ou reiniciar a mesma.

4.4.18.14. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).

4.4.18.15. Deverá oferecer a possibilidade de armazenar backups de forma criptografada, bem como garantir o trânsito de informações sob esse esquema a partir do arquivo de backup, sem exigir criptografia do sistema de armazenamento.

4.4.18.16. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar.

4.4.18.17. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.

4.4.18.18. Deverá permitir criar uma cópia da máquina virtual de produção para criação de ambiente de homologação, testes ou desenvolvimento, em qualquer estado anterior, para a resolução de problemas, provas de procedimentos ou capacitação.

4.4.18.19. Deverá permitir a recuperação de mais de uma máquina virtual e pontos de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.

4.4.18.20. O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup.

4.4.18.21. O software deverá permitir a execução de backup de arquivos abertos em Windows, mesmo que estejam sendo alterados durante a operação e backup, sem necessidade de suspender a utilização de aplicações pelos usuários nem a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup.

4.4.18.22. O sistema deve prover quantidade ilimitada de restaurações, conforme as solicitações da CONTRATANTE, durante a vigência deste Contrato.

4.4.18.23. O console central de administração dos backups das máquinas virtuais deve ser via WEB e acessível via navegador utilizando protocolos HTTPS integrado a solução de Console de gestão do ambiente Cloud Computing.

4.4.18.24. Solução de backup para caixas de correio do Office365, conforme características abaixo:

4.4.18.25. O painel de administração do backup e restore das caixas de correio poderá ser separado da administração dos backups das máquinas virtuais, porém deverá ser da mesma fabricante.

4.4.19. RECUPERAÇÃO DE DESASTRES

4.4.19.1. Deverá fornecer solução de recuperação de desastres, baseado em replicação automatizada entre os datacenters da CONTRATADA.
4.4.19.2. A solução deverá ser integrada a mesma solução de gerenciamento do ambiente de máquinas virtuais, não sendo permitido utilização de software externos.
4.4.19.3. Garantir a proteção e replicação automatizada de máquinas virtuais.
4.4.19.4. Permitir a criação de planos de recuperação personalizáveis.
4.4.19.5. Deverá possuir funcionalidade de testes de plano de recuperação sem impacto.
4.4.19.6. Permitir a recuperação orquestrada quando necessário.
4.4.19.7. Permitir a replicação e recuperação para outro ambiente de Cloud Computing.
4.4.19.8. Permitir a utilização do ambiente em nuvem como datacenter secundário ou como um ambiente de recuperação.
4.4.19.9. Fornecer o monitoramento e envio de alertas do estado de suas instâncias protegidas.
4.4.19.10. A solução deverá permitir a reconfiguração das interfaces de rede destino.
4.4.19.11. A solução deverá disponibilizar a réplica de armazenamento em um segundo datacenter isolado do armazenamento de origem.
4.4.19.12. O armazenamento disponível para as maquinas virtuais replicadas deverão considerar o armazenamento dos dados de forma persistente.
4.4.19.13. O armazenamento da réplica disponível deverá permitir que a CONTRATANTE defina através de políticas pré existentes a seguinte carga de uso:
4.4.19.13.1. ALTA PERFORMANCE (SSD)
4.4.19.13.2. BAIXA PERFORMANCE (HDD)
4.4.19.14. Solução de Desastre Padrão
4.4.19.14.1. A solução de desastres padrão deverá ser licenciada por máquina virtual.
4.4.19.14.2. A solução de desastre padrão deverá ser entregue com uma política de replicação a cada 24 horas.
4.4.19.15. Solução de Desastres Avançado
4.4.19.15.1. A solução de desastre avançada deverá ser licenciada por máquina virtual.
4.4.19.15.2. A solução de desastre avançada deverá ser entregue com uma política de replicação para no mínimo 15 minutos de RPO (Recovery Point Object).
4.4.19.15.3. A solução de desastre avançada deverá ser entregue com a funcionalidade de retenção para os pontos no tempo, provendo no mínimo 7 dias de retenção.

4.4.20. SOLUÇÃO DE DETECÇÃO E REPOSTA DE ENDPOINT
4.4.20.1. Requisitos gerais da solução:
4.4.20.1.1. Solução de proteção contra ameaças avançadas, com funcionalidades de detecção, bloqueio, investigação e resposta a incidentes, incluindo console Web ou console gráfica do próprio fabricante para administração da solução e centralização de eventos.
4.4.20.1.2. Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento
4.4.20.1.3. A Solução de gerência deve ser fornecida pela licitante vencedora e contemplar todos os softwares e respectivas licenças necessárias ou adicionais para a instalação, configuração e funcionamento da solução de proteção.
4.4.20.1.4. A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.
4.4.20.1.5. Na data da proposta, nenhum dos softwares componentes da solução de proteção ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“end of support”) ou fim de vendas (“end of sale”).
4.4.20.1.6. Deverá ser considerado o licenciamento para 25 dispositivos pelo período do contrato.
4.4.20.2. Requisitos e funcionalidades técnicos da solução:
4.4.20.2.1. A solução de proteção deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zeroday), ataques file-less, ameaças persistentes avançadas (APTs), ransomwares, exploits e outros comportamentos maliciosos, sem depender exclusivamente de base de assinaturas ou heurísticas.

4.4.20.2.2. A solução de proteção deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares com capacidade de restauração dos arquivos comprometidos.
4.4.20.2.3. A solução de proteção deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações.
4.4.20.2.4. A solução de proteção deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades.
4.4.20.2.5. Efetuar a análise baseada em técnicas de machine learning, inteligência artificial e threat intelligence, permitindo a proteção contra ataques que explorem vulnerabilidades, mesmo que ainda não existam patches de correção.
4.4.20.2.6. Realizar análise de comportamento com base nas táticas, técnicas e procedimentos (TTPs) listados no framework MITRE ATT&CK.
4.4.20.2.7. A análise dos artefatos deve ocorrer em pré-execução, ou seja, antes de serem executados no sistema operacional, evitando que a máquina seja infectada.
4.4.20.2.8. Detectar e bloquear ameaças que utilizem técnicas de ofuscação e sequestro de DLL.
4.4.20.2.9. Detectar e bloquear técnicas de evasão, incluindo process injection e uso de executáveis legítimos do Windows para rodar scripts e ações maliciosas.
4.4.20.2.10. Reconhecer padrões e bloquear comportamentos potencialmente maliciosos ou o possuir mecanismos automáticos preventivos ou corretivos que sejam capazes de inibir as ações maliciosas resultantes de pelo menos 5(cinco) das ações listadas abaixo:
4.4.20.2.11. Rodar a partir diretórios incomuns (ex: diretório de dados, temp e lixeira);
4.4.20.2.12. Executar elevações de privilégio inesperadas;
4.4.20.2.13. Tentar se passar por processos do Windows;
4.4.20.2.14. Estabelecer conexões de rede suspeitas (call back ou command & control);
4.4.20.2.15. Uso suspeito do PSEXEC;
4.4.20.2.16. Invocação maliciosa através do Rundll;
4.4.20.2.17. Exploração ou modificação do arquivo hosts;
4.4.20.2.18. Tentativa de invocação de Remote Shell.
4.4.20.2.19. Identificar e bloquear alterações suspeitas em chaves de registro e tarefas agendadas na máquina.
4.4.20.2.20. Proteger contra macros maliciosas, bem como scripts e comandos Powershell maliciosos.
4.4.20.2.21. Bloquear exploits e payloads suspeitos do Metasploit.
4.4.20.2.22. As análises poderão ser complementadas utilizando recursos em nuvem da solução, sem custos adicionais, onde será permitido apenas o envio de metadados dos artefatos sob análise, sem submissão do artefato em si ou seu conteúdo à nuvem.
4.4.20.2.23. O agente da solução deve realizar suas análises e bloqueios nas estações mesmo quando estiver sem conectividade com os servidores da solução e sem acesso à Internet.
4.4.20.2.24. O agente da solução deve possuir proteção contra desinstalação e/ou desativação dos seus componentes, serviços e processos de forma não autorizada.
4.4.20.2.25. Deve ser possível realizar a configuração de proxy no agente ou obter as configurações de proxy definidas no próprio sistema operacional.
4.4.20.2.26. Deve ser possível exibir ou inibir alertas ao usuário em caso de detecção de alguma ameaça, conforme definição do administrador.
4.4.20.2.27. Deve ser possível definir as seguintes ações de resposta quando uma ameaça ou comportamento malicioso for detectado:
4.4.20.2.28. Ignorar;
4.4.20.2.29. Registrar em log;
4.4.20.2.30. Alertar;
4.4.20.2.31. Bloquear;
4.4.20.2.32. Remover ou quarentenar;
4.4.20.2.33. Isolar a máquina, de maneira que ela perca a comunicação com a rede ou se

comunique apenas com os servidores da solução ou com servidores e serviços definidos na política de isolamento.

4.4.20.2.34. I - O agente deve ter a capacidade de fazer o isolamento da máquina por si só, sem precisar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

4.4.20.2.35. II - Deve ser possível ao administrador efetuar a liberação da máquina do isolamento via console de gerência ou fornecer uma chave para realizar a liberação.

4.4.20.2.36. A solução deve possuir funcionalidade de EDR e análise forense, provendo uma visão completa do fluxo do ataque e informações detalhadas sobre os comportamentos detectados, de forma a auxiliar e agilizar as ações de remediação.

4.4.20.2.37. A console deve oferecer uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

4.4.20.2.38. Devem ser coletadas as atividades de todos artefatos analisados, contendo informações sobre interação com outros processos, arquivos e chaves de registro acessadas /modificadas, conexões de rede realizadas, dentre outras. Deve ser possível gerar relatório dessas informações.

4.4.20.2.39. A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.

4.4.20.2.40. Deve ser possível configurar regras de exclusão (whitelists) determinando quais arquivos, diretórios, processos ou aplicativos não devem ser analisados pela solução.

4.4.20.2.41. A solução deve ser capaz de remover de forma ágil e eficaz outras soluções de antivírus instaladas nos equipamentos do CONTRATANTE ou possuir mecanismos que possibilitem essa remoção.

4.4.20.2.42. A Solução deve ter a capacidade de implementar, no mínimo, cinco das seguintes funcionalidades:

4.4.20.2.43. Reputação de Arquivos (Com ou sem acesso à internet no endpoint);

4.4.20.2.44. IPS de Próxima Geração;

4.4.20.2.45. Proteção de Navegadores;

4.4.20.2.46. Aprendizado de Máquinas;

4.4.20.2.47. Análise Comportamental;

4.4.20.2.48. Mitigação da Exploração de Memória;

4.4.20.2.49. Controle e isolamento de Aplicações;

4.4.20.2.50. Controle de Dispositivos;

4.4.20.2.51. Emulação para Malware;

4.4.20.2.52. Proteção ao ambiente de Active Directory;

4.4.20.2.53. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas.

4.4.20.2.54. Deve ter a capacidade de implementar a funcionalidade de “Machine Learning” utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos.

4.4.20.2.55. De forma opcional ou não obrigatória a solução poderá a solução poderá ser capaz de distribuir iscas no ambiente com o objetivo de detectar e interromper tentativas de infiltração, através da implementação de pelo menos:

4.4.20.2.56. Criação de entradas falsas de cache, como Cache de DNS afim de enganar um invasor e identificar ações maliciosas no ambiente;

4.4.20.2.57. Deve possibilitar a criação de arquivos falsos nas máquinas dos usuários;

4.4.20.2.58. Deve possibilitar a criação e distribuição de senhas falsas nos sistemas afim de identificar invasores no ambiente;

4.4.20.2.59. Criação de compartilhamentos de rede falsos em desktops;

4.4.20.2.60. Deve ser capaz de enviar alertas quando as “Iscas” falsas são acionadas e/ou modificadas;

4.4.20.2.61. Deve ter a capacidade de revelar tentativas de ataques dentro da rede interna;

4.4.20.2.62. De forma opcional ou não obrigatória, a solução poderá ter a capacidade de impedir

os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo um dos conhecidos comportamentos de exploração de vulnerabilidades:
4.4.20.2.63. SEHOP - Structured Exception Handler Overwrite Protection;
4.4.20.2.64. Heap Spray (Exploits que iniciam através do HEAP);
4.4.20.2.65. Java Exploit Protection;
4.4.20.2.66. De forma opcional ou não obrigatória, a solução poderá se capaz de:
4.4.20.2.67. A solução poderá ter a capacidade de bloquear exploits que trabalham em nível de “shell code”.
4.4.20.2.68. A solução poderá ter proteção contra técnicas de reconhecimento do domínio, sendo capaz de detectar um invasor que utilize técnicas de movimentação lateral ou roubo de credenciais válidas;
4.4.20.2.69. A solução poderá proteger contra intrusões por processo, usuário e terminal;
4.4.20.2.70. A solução poderá ser capaz de identificar vulnerabilidades, erros de configurações e possíveis Backdoors presentes no Active Directory;
4.4.20.2.71. A solução poderá ser capaz de proteger alterações no Active Directory sem a necessidade de instalação de agentes ou componentes adicionais nas estações de trabalho;
4.4.20.2.72. A solução poder ser capaz de detectar e proteger roubos de credenciais no ambiente que utilizem a técnica Pass-the-Hash e Pass-the-Ticket;
4.4.20.2.73. Instalação dos agentes:
4.4.20.2.74. A solução deve ser compatível com as versões de Sistema Operacionais:
4.4.20.2.75. Para computadores de usuários finais (estações: desktop, workstation e notebooks):
4.4.20.2.76. I - Microsoft Windows 7 (32-64bit) e superior em todas as suas distribuições (home, starter, professional, ultimate e enterprise).
4.4.20.2.77. Para servidores de rede físicos ou virtuais:
4.4.20.2.78. I - Microsoft Windows Server 2012 (64bit) e superior.
4.4.20.2.79. II - Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux, Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).
4.4.20.2.80. IV - O agente deve suportar sua instalação em Sistemas Operacionais virtualizados em ambiente Vmware.
4.4.20.2.81. O agente não deve impactar a performance das estações e servidores, gerando baixo consumo de CPU, memória, disco e rede.
4.4.20.2.82. Deve ser possível a instalação e atualização dos agentes de forma manual ou remota, com suporte à distribuição do agente por ferramentas de terceiros, incluindo o System Center Configuration Manager (SCCM) da Microsoft.
4.4.20.2.83. A instalação deve ser feita de forma silenciosa, sem interação com o usuário e sem necessidade de acesso à Internet.
4.4.20.2.84. Deve ser possível permitir a desinstalação ou alteração da configuração do agente mediante requisição de senha ou token gerados pela console de gerência.
4.4.20.2.85. Deve ser possível impedir alterações na configuração do agente por usuários ou processos não autorizados.
4.4.20.2.86. Toda a solução deverá funcionar com agente único na estação de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final;
4.4.20.2.87. Para equipamentos que não podem se conectar à internet, devido a regras de negócio e/ou restrições impostas pelo próprio equipamento, a solução deve possibilitar a instalação de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.
4.4.20.2.88. Toda a solução deverá funcionar com agente nas estações de trabalho e servidores físicos e/ou virtuais a fim de diminuir o impacto ao usuário final. Será permitido agentes múltiplos para o atendimento deste requisito.
4.4.20.2.89. Console de Gerência:
4.4.20.2.90. A solução deve oferecer console de gerência via protocolo web seguro ou console do próprio fabricante.
4.4.20.2.91. Caso a console seja Web, deve ser compatível com pelo menos dois dos seguintes

navegadores: Microsoft Edge 41 ou superior; Google Chrome 70 ou superior; Mozilla Firefox 60 ou superior.
4.4.20.2.92. A console deve funcionar plenamente sem requerer a instalação de plug-ins, drivers, java e flash player.
4.4.20.2.93. Permitir no mínimo 5(cinco) acessos simultâneos.
4.4.20.2.94. A console e os agentes da solução devem possuir interface em português ou inglês.
4.4.20.2.95. Toda comunicação da solução deve ocorrer de forma criptografada usando protocolo seguro conforme padrão aceito pela indústria.
4.4.20.2.96. Permitir a configuração de perfis com permissões agrupadas que possam ser vinculados às contas de acesso à solução, para possibilitar a segregação de funções.
4.4.20.2.97. Suporte à criação de usuários, permitindo senhas de no mínimo 8 caracteres de 3 ou mais tipos, como: letras maiúsculas, letras minúsculas, dígitos numéricos e caracteres especiais.
4.4.20.2.98. A solução de console de gerência, deve ser possível configurar autenticação em múltiplos fatores.
4.4.20.2.99. Permitir ao administrador criar diferentes políticas de segurança e aplicá-las a diferentes grupos de máquinas de acordo com seus atributos.
4.4.20.2.100. Registro em log de todas as ações de detecção e bloqueio de malware e comportamento malicioso.
4.4.20.2.101. Deve ser possível efetuar busca no log pelo IP de Origem, IP de destino, nome da máquina, nome do processo, arquivo e chave de registro.
4.4.20.2.102. Deve ser possível efetuar o “drill down” das consultas realizadas afim de avaliação mais detalhada das ocorrências.
4.4.20.2.103. A partir dos eventos exibidos na console, deve ser possível tomar ações como quarentenar a máquina, adicionar o artefato a blacklist ou lista de exclusão (whitelist), dentre outras.
4.4.20.2.104. Permitir a geração de relatórios, consulta em log ou dashboard para visualizar no mínimo as informações abaixo:
4.4.20.2.105. Eventos de ameaças;
4.4.20.2.106. Eventos de comportamentos suspeitos;
4.4.20.2.107. Malwares detectados e bloqueados;
4.4.20.2.108. Computadores infectados.
4.4.20.2.109. Deve ser possível exportar os relatórios para o formato CSV ou PDF.
4.4.20.2.110. Permitir a configuração de alertas em tempo real de ameaças com envio de e-mail a usuários pré-definidos.
4.4.20.2.111. A solução deve manter log de auditoria com registro das configurações realizadas por qualquer usuário ou administrador do sistema.
4.4.20.2.112. Permitir a visualização do inventário das máquinas que possuem o agente instalado, contendo no mínimo as seguintes informações:
4.4.20.2.113. Nome da máquina;
4.4.20.2.114. Endereço IP;
4.4.20.2.115. Versão do sistema operacional (incluindo a versão do Service Pack);
4.4.20.2.116. Versão do agente;
4.4.20.2.117. Política aplicada.
4.4.20.2.118. A partir do console de gerenciamento da solução, deve ser possível identificar o equipamento que está sofrendo ataques e comandar o agente de endpoint para que aquele determinado equipamento seja movido para uma área de quarentena.
4.4.20.2.119. Monitoramento Assistido:
4.4.20.2.120. Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do CONTRATANTE.
4.4.20.2.121. Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;
4.4.20.2.122. Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);

4.4.20.2.123. Este serviço deverá ser prestado por equipe própria da CONTRATADA ou pela fabricante da solução;
4.4.20.2.124. Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;
4.4.20.2.125. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
4.4.20.2.126. A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, está não deverá atingir períodos superiores a 4 horas consecutivas;
4.4.20.2.127. A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;
4.4.20.2.128. O serviço deverá atender os seguintes requisitos:
4.4.20.2.129. Monitorar ferramentas de segurança;
4.4.20.2.130. Monitorar o armazenamento dos logs de eventos e e incidentes de segurança;
4.4.20.2.131. Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;
4.4.20.2.132. Iniciar tratamento de incidentes em até 10 min;
4.4.20.2.133. Realizar triagem, classificação e categorização de eventos de segurança da informação;
4.4.20.2.134. Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;
4.4.20.2.135. Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;
4.4.20.2.136. Registrar, escalar e notificar incidentes de segurança da informação;
4.4.20.2.137. Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;
4.4.20.2.138. Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;
4.4.20.2.139. Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;
4.4.20.2.140. Registrar e documentar ações e procedimentos realizados;
4.4.20.2.141. Emitir relatório semanal estatístico das operações realizadas;
4.4.20.2.142. Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;
4.4.20.2.143. Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;
4.4.20.2.144. Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;
4.4.20.2.145. Apoiar na definição, documentação e manutenção da normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE , visando refletir as definições instituídas por esses serviços de monitoramento;
4.4.20.2.146. Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;
4.4.20.2.147. Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;
4.4.20.2.148. Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.

4.4.20.2.149. Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;
4.4.20.2.150. Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;
4.4.20.2.151. Gerar subsídios e recomendações para elaboração de conteúdo para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;
4.4.20.2.152. Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;
4.4.20.2.153. Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.
4.4.20.2.154. Instalação da solução e repasse de conhecimento
4.4.20.2.155. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser realizada pela Contratada ou pelo fabricante da solução presencialmente na Sede do CONTRATANTE, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.
4.4.20.2.156. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deve ser executada por pessoal especializado, qualificado e com certificação na solução.
4.4.20.2.157. A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do CONTRATANTE e em até 60 (sessenta) dias corridos para as unidades nas demais localidades, contados a partir da assinatura da Ordem de Serviço, conforme item 6.1.1.
4.4.20.2.158. A instalação compreenderá:
4.4.20.2.159. Implantação de todos os componentes em sua última versão estável.
4.4.20.2.160. Configuração completa da solução, incluindo o apoio na definição de políticas e melhores práticas de segurança.
4.4.20.2.161. Configuração de dashboards, relatórios e alertas, de maneira coordenada com o CONTRATANTE.
4.4.20.2.162. Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do CONTRATANTE, inclusive nas unidades descentralizadas nos estados da federação.
4.4.20.2.163. Instrução da equipe técnica do CONTRATANTE para a integração da a solução com ferramenta SIEM ou envio para servidor de registro de logs (Syslog).
4.4.20.2.164. Documentação da topologia da solução, relatório das atividades e configurações realizadas.
4.4.20.2.165. Apresentação da solução configurada e implantada.
4.4.20.2.166. Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupo de até 4 pessoas, oferecido por técnico certificado na solução.
4.4.20.2.167. No repasse de conhecimento deve ser utilizado material em português.
4.4.20.2.168. Não é necessário que o repasse seja feito para um grupo fechado do CONTRATANTE e o mesmo pode ser realizado de forma remota.
4.4.20.2.169. O repasse de conhecimento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes, introdução ao Framework MITRE ATT&CK e outros.
4.4.20.2.170. As datas dos repasses de conhecimento devem ser previamente combinadas com o CONTRATANTE.
4.4.20.2.171. Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.
4.4.20.2.172. Caso o repasse de conhecimento seja ministrado presencialmente e fora de São

Paulo, deverão estar incluídas as despesas com passagens aéreas, hospedagem e traslado entre aeroporto, hotel e local de treinamento.
4.4.20.2.173. O CONTRATANTE se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária. Neste caso, eventuais despesas de locomoção e estadia serão ressarcidas ao CONTRATANTE pela Contratada.
4.4.20.2.174. Deverá ser disponibilizado formulário de avaliação (online ou impresso) e a média das notas deverá ser superior a 80%. Caso a média das notas seja inferior a 80% a contratada deverá ministrar novo repasse.
4.4.20.2.175. A fornecedora e/ou fabricante da solução poderá, a qualquer tempo, durante a vigência do contrato, sem ônus extra para o CONTRATANTE, oferecer participação em seminários, conferências, visitas técnicas, eventos educacionais e treinamentos não previstos nesta especificação técnica, desde que relacionados ao objeto contratado.

4.4.21. OPERAÇÃO, SUPORTE E GERENCIAMENTO

4.4.21.1. A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.
4.4.21.2. É responsabilidade da CONTRATADA monitorar a solução 24 x 7 x 365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.
4.4.21.3. A CONTRATADA será responsável por operar e gerenciar as tarefas de backup de acordo com as solicitações realizadas pelo time da CONTRATANTE, devendo adicionar, alterar ou remover tarefas e rotinas de backup, de acordo com as solicitações.
4.4.21.4. A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup.
4.4.21.5. Em casos de falha, a CONTRATADA deverá notificar prontamente o time da CONTRATANTE, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.
4.4.21.6. A CONTRATANTE terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup sem qualquer custo adicional.
4.4.21.7. A CONTRATADA deverá enviar mensalmente relatório estatístico das rotinas de backup.
4.4.21.8. A CONTRATADA deverá fornecer suporte técnico na modalidade 8 x 5 (8 horas por dia e 5 dias por semana) em língua portuguesa, para sanar dúvidas quanto da solução, sua configuração ou quaisquer outros assuntos relacionados à solução, através de suporte telefônico, por e-mail e através de um sistema online de chamados.
4.4.21.9. Em casos de acionamento de desastre, restaurações de bancos ou que seja necessária a restauração baremetal de um ou mais servidores, a CONTRATADA deve disponibilizar time técnico devidamente qualificado e de forma presencial nas dependências da CONTRATADA para a realização ou acompanhamento das tarefas.
4.4.21.10. A equipe técnica deverá estar alocada em até no máximo 4 horas na CONTRATANTE, após a constatação efetiva do desastre.
4.4.21.11. Durante a execução deste serviço a CONTRATADA se obriga a manter profissional (ais) com todas as qualificações.

4.4.22. PROVISIONAMENTO DO AMBIENTE CLOUD COMPUTING

4.4.22.1. A CONTRATADA será responsável por criar os novos servidores no ambiente de Cloud Computing, com as versões do sistema operacional e dos softwares básicos especificados pela CONTRATANTE.
4.4.22.2. Será de responsabilidade da equipe técnica da CONTRATADA, com o apoio da equipe técnica da CONTRATANTE, a migração das aplicações para o novo ambiente, sendo que a CONTRATANTE disponibilizará os recursos necessários, tanto de equipamentos quanto humanos, para apoiar a migração das aplicações.
4.4.22.3. Será de responsabilidade da equipe técnica da CONTRATADA o acompanhamento e auxilio a instalação dos softwares básicos e a migração das aplicações da CONTRATANTE, durante a migração a CONTRATANTE disponibilizará o conhecimento da estrutura das aplicações

e dos softwares básicos necessários (programas, diretórios, arquivos de configuração e demais informações) para a CONTRATADA afim de otimizar os recursos.
4.4.22.4. Após a finalização da migração das aplicações para o ambiente Cloud Computing, a CONTRATANTE disponibilizará uma equipe técnica para fazer os testes de homologação das aplicações migradas afim de atestar a conclusão da migração, sendo que os serviços contratados somente serão considerados como entregues aceitos após a conclusão dos testes.

4.5. CONDIÇÕES GERAIS

4.5.1. Permitir que os técnicos designados pela contratada, tenham pleno acesso ao(s) equipamento(s) a fim de executar os serviços de manutenção, objeto deste contrato, na presença de pessoa autorizada pela contratante.
4.5.2. Cada uma das partes deverá designar um funcionário para intermediar o relacionamento contratual com vistas a fiscalizar, e controlar a execução dos Serviços e uso de peças de reposição.
4.5.3. A parte que substituir o funcionário por ela designado deverá comunicar o fato imediatamente à outra parte.

Requisitos de Capacitação

4.6. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

Requisitos Legais

4.7. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei n° 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

Requisitos de Experiência Profissional

4.8. Por se tratar de serviço que requer de seu executor conhecimentos técnicos especializados em face do grau de complexidade envolvida, o licitante vencedor deverá comprovar, através de atestado (s), declaração(ões) ou certidão(ões) de capacidade técnica expedido(s) por pessoa jurídica, de direito público ou privado, que comprove a aptidão para comercialização e implementação de Firewall baseado em appliance, visando assegurar a CONTRATANTE atender efetivamente os serviços pretendidos e descritos neste Termo de Referência.

Requisitos de Formação da Equipe

4.9. Em virtude da grande complexidade técnica do ambiente em produção na Fundação Casa, por se tratar de um ambiente em produção com aplicações críticas, bem como a fim de garantir a competência técnica para prestar os serviços objeto desta contratação, a licitante deverá comprovar que possui em seu quadro de colaboradores no mínimo 2 (dois) profissionais técnicos certificados pelo fabricante Dell nas áreas de servidores, storage e redes (network), além de 1 (um) profissional técnico certificado pelo fabricante Fortinet nas áreas de firewall.

5. Papéis e responsabilidades

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

5.2. São obrigações do CONTRATADO

5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5.. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.9. fazer a transição contratual, quando for o caso;

6. Modelo de execução do contrato

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: 05 dias da emissão da ordem de serviço.

Local da prestação dos serviços

6.2. Os serviços serão prestados no seguinte endereço: Sede Administrativa - Rua Florêncio de Abreu, 848, 9º andar, Luz, São Paulo - SP, CEP: 01030-001, observando o horário de funcionamento da instituição.

Especificação da garantia do serviço

6.3. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 36 (trinta e seis) meses, contados a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

Formas de transferência de conhecimento

6.4. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

6.5. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Manutenção de Sigilo e Normas de Segurança

6.6. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

7. Modelo de gestão do contrato

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

Fiscalização

7.9. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

7.10. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto estadual nº 68.220, de 2023, art. 17).

7.11. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133, de 2021, art. 117, § 1º e Decreto estadual nº 68.220, de 2023, art. 17, II).

7.12. O fiscal técnico realizará, em conformidade com cronograma físico-financeiro, as medições dos serviços executados e aprovará a planilha de medição emitida pelo Contratado (Decreto estadual nº 68.220, de 2023, art. 17, III).

7.13. O fiscal técnico adotará medidas preventivas de controle de contratos, manifestando-se quanto à necessidade de suspensão da execução do objeto (Decreto estadual nº 68.220, de 2023, art. 17, IV).

7.14. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso (Lei federal nº 14.133, de 2021, artigo 117, § 2º).

7.15. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato (Decreto estadual nº 68.220, de 2023, art. 17, II).

Fiscalização Administrativa

7.16. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Decreto estadual nº 68.220, de 2023, art. 18, II e III).

7.17. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência (Decreto estadual nº 68.220, de 2023, art. 18, IV).

7.18. Sempre que solicitado pelo Contratante, o Contratado deverá comprovar o cumprimento da reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, com a indicação dos empregados que preencherem as referidas vagas, nos termos do parágrafo único do artigo 116 da Lei nº 14.133, de 2021.

Gestor do Contrato

7.19. O gestor do contrato exercerá a atividade de coordenação dos atos de fiscalização técnica, administrativa e setorial e dos atos preparatórios à instrução processual visando, entre outros, à prorrogação, à alteração, ao reequilíbrio, ao pagamento, à eventual aplicação de sanções e extinção do contrato (Decreto estadual nº 68.220, de 2023, inciso I do art. 2º).

7.20. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais (Decreto estadual nº 68.220, de 2023, art. 16, IX).

7.21. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações (Decreto estadual nº 68.220, de 2023, art. 18, VII).

7.22. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto estadual nº 68.220, de 2023, art. 16, VIII).

7.23. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração (Decreto estadual nº 68.220, de 2023, art. 16, VII e parágrafo único).

7.24. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato

Critérios de medição e pagamento

7.25. A avaliação da execução do objeto observará o disposto nesta seção.

7.26. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

7.26.1. não produzir os resultados acordados;

7.26.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

7.26.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

Do recebimento

7.27. Os serviços serão recebidos provisoriamente, no prazo de 04 (quatro) dias úteis, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

7.27.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

7.28. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

7.29. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

7.30. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

7.31. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.31.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

7.32. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.33. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

7.34. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.35. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.36. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

7.37. Os serviços serão recebidos definitivamente no prazo de 04 (quatro) dias úteis, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

7.37.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

7.37.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

7.37.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

7.37.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.37.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.38. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.39. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.40. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

7.41. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, a contar de seu recebimento pela Administração, na forma desta seção, prorrogáveis por igual período, justificadamente, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais (art. 7º, I, e §§ 2º e 3º, da Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, c/c o Decreto estadual nº 67.608, de 2023).

7.42. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

7.43. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

7.43.1. o prazo de validade;

7.43.2. a data da emissão;

7.43.3. os dados do contrato e do órgão contratante;

7.43.4. o período respectivo de execução do contrato;

7.43.5. o valor a pagar; e

7.43.6. eventual destaque do valor de retenções tributárias cabíveis.

7.44. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

7.45. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.46. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

7.47. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua

situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

7.48. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.49. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

7.50. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

7.51. O pagamento será efetuado no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal ou documento de cobrança equivalente, desde que tenha sido finalizada a liquidação da despesa, conforme seção anterior, nos termos do art. 2º, inciso II, do Decreto estadual nº 67.608, de 2023.

7.52. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente na forma da legislação aplicável (art. 2º, inciso III, do Decreto estadual nº 67.608, de 2023, c/c o art. 1º do Decreto estadual nº 32.117, de 1990), bem como incidirão juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados pro rata temporis, em relação ao atraso verificado.

Forma de pagamento

7.53. O pagamento será realizado por meio de ordem bancária, para depósito em conta corrente bancária em nome do Contratado no Banco do Brasil S/A.

7.53.1. Constitui condição para a realização dos pagamentos a inexistência de registros em nome do Contratado no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pelo Contratado, de que os registros estão suspensos, nos termos do art. 8º da Lei estadual nº 12.799, de 2008.

7.54. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.55. O Contratante poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

7.55.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente

7.56. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. Do reajuste

8.1 Em conformidade com o inciso I do § 8º do art. 25 da Lei nº 14.133, de 2021, nas hipóteses de contratação de serviços contínuos sem regime de dedicação exclusiva de mão de obra e sem predominância de mão de obra, aplica-se a disciplina de reajustamento em sentido estrito, nos termos do inciso IV do art. 2º do Decreto estadual nº 67.608, de 2023, baseada no IPC-FIPE - Índice de Preços ao Consumidor elaborado pela Fundação Instituto de Pesquisas Econômicas da Universidade de São Paulo.

9. Critérios de seleção do fornecedor

Forma de seleção e critério de julgamento da proposta

9.1. *O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO e modo de disputa ABERTO.*

Regime de Execução

9.2. O regime de execução do contrato será de empreitada por preço global.

Da Aplicação da Margem de Preferência

9.3. Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

9.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos das seções subsequentes deste item 8, que serão exigidos conforme sua natureza jurídica:

Habilitação jurídica

9.5. **Empresário individual**: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.6. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

9.7. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.8. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

9.9. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.10. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

9.11. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

9.12. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

9.13. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.14. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.15. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.16. Prova de inscrição no cadastro de contribuintes Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.17. Prova de regularidade com a Fazenda Municipal/Distrital quanto ao Imposto sobre Serviços de Qualquer Natureza – ISSQN, do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.18. Caso o fornecedor se considere isento ou imune de tributos relacionados ao objeto contratual, em relação aos quais seja exigida regularidade fiscal neste instrumento, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.19. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

9.20. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de sociedade simples;

9.21. Certidão negativa de falência, expedida pelo distribuidor da sede do fornecedor, caso se trate de empresário individual ou sociedade empresária;

9.22. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um).

9.22.1. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (Lei nº 14.133, de 2021, art. 65, § 1º).

9.22.2. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

9.22.3. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped, quando for o caso, ou outro limite estabelecido pela legislação aplicável.

9.23. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

9.24 Comprovação de capacidade para execução de serviço similar de complexidade tecnológica e operacional equivalente ou superior aos serviços a serem contratados, mediante a apresentação de de certidão(ões) ou atestado(s), fornecido(s) por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso, que demonstrem, ao menos os seguintes elementos:

a) aptidão para comercialização e implementação de Firewall baseado em appliance;

b) deverá haver a comprovação da experiência mínima de 1 (um) ano na prestação de serviços similares, sendo aceito o somatório de atestados ou certidões de períodos diferentes, não havendo obrigatoriedade de os anos serem ininterruptos.

9.24.1. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do licitante;

9.24.2. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do (s) atestado(s), apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o objeto contratado, dentre outros documentos;

Outras comprovações

9.25. Declaração subscrita por representante legal do licitante, atestando que:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do art. 117, parágrafo único, da Constituição Estadual;

b) atenderá, na data da contratação, ao disposto no art. 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no art. 5º-D, ambos da Lei nº 6.019, de 1974, com redação dada pela Lei nº 13.467, de 2017, quando o caso;

9.26. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que possui em seu quadro de colaboradores, no mínimo, 02 (dois) profissionais técnicos certificados pelo fabricante Dell nas áreas de servidores, storage e redes (network), além de 1 (um) profissional técnico certificado pelo fabricante Fortinet nas áreas de firewall.

9.27. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia e assistência técnica para os equipamentos listados no Anexo I.1 – parte A, deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

9.28. Declaração subscrita por representante legal do licitante, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware listados no Anexo I.1 – parte C serão prestados pelo próprio fabricante (Vmware e Fortinet), para todas as licenças existentes na Fundação CASA.

8.29. **Tratando-se de consórcio**:

8.29.1. Apresentação do compromisso público ou particular de constituição do consórcio, subscrito pelos consorciados, o qual deverá incluir, pelo menos, os seguintes elementos:

a) Designação do consórcio e sua composição;

b) Finalidade do consórcio;

c) Prazo de duração do consórcio, que deve coincidir, no mínimo, com o prazo de vigência contratual;

d) Endereço do consórcio e o foro competente para dirimir eventuais demandas entre os consorciados;

e) Definição das obrigações e responsabilidades de cada consorciado e das prestações específicas;

f) Previsão de responsabilidade solidária de todos os consorciados pelos atos praticados pelo consórcio, tanto na fase de licitação quanto na de execução do contrato, abrangendo também os encargos fiscais, trabalhistas e administrativos referentes ao objeto da contratação;

g) Indicação da empresa líder do consórcio e seu respectivo representante legal, que deverá ter poderes para receber citação, interpor e desistir de recursos, firmar a contratação e praticar todos os demais atos necessários à participação na licitação e execução do objeto contratado, sendo responsável pela representação do consórcio perante a Administração;

h) Compromisso subscrito pelas consorciadas de que o consórcio não terá a sua composição modificada sem a prévia e expressa anuência do Contratante até o integral cumprimento do objeto da contratação, observado o prazo de duração do consórcio, definido na alínea “c” deste subitem;

8.29.2. O licitante vencedor é obrigado a promover, antes da celebração da contratação, a constituição e o registro do consórcio, nos termos de seu compromisso de constituição.

8.29.3. Cada consorciado, individualmente, deverá atender as exigências relativas a habilitação jurídica e habilitação fiscal, social e trabalhista, e a certidão negativa de falência/insolvência. Para efeito de habilitação econômico-financeira e de habilitação técnica, quando exigida, será observado o disposto no inciso III do caput do art. 15 da Lei nº 14.133, de 2021;

8.29.4. Para efeito de habilitação econômico-financeira e de habilitação técnica, quando exigida, será observado o disposto no inciso III do caput do artigo 15 da Lei federal nº 14.133/2021.

8.29.5. A inabilitação de qualquer consorciado acarretará a automática inabilitação do consórcio.

8.30. **Tratando-se de cooperativas**, será exigida a seguinte documentação complementar, para evidenciar a observância do disposto no artigo 16 da Lei federal nº 14.133/2021:

8.30.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

8.30.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

8.30.3. Regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

8.30.4. Edital de convocação e ata da última assembleia geral, e registro de presença dos cooperados presentes nessa assembleia;

8.30.5. Ata da reunião em que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

8.30.6. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

8.30.7. Documentação que seja demonstrativa de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados, caso essa circunstância não esteja evidenciada na documentação a ser apresentada para atendimento aos subitens anteriores.

10. Estimativas do valor da contratação

[Conteúdo Sigiloso | Justificativa: 9.1 O art. 24 da Lei nº 14.133/2021 concede a discricionariedade para a Administração Pública, desde que justificado, a opção de adotar o caráter sigiloso do orçamento estimado da contratação, sem prejuízo do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas. Não prevalecendo, para tanto os órgãos de controle interno e externo. 9.2 Com fundamento no referido artigo, opta-se pela adoção do caráter sigiloso do orçamento destinado para a contratação, uma vez que tal modalidade possibilita maior atendimento aos princípios que regem a Administração Pública, como o da competividade, eficiência e da economicidade, conforme artigo 5º da lei ora mencionada. 9.3 O orçamento estimado com caráter sigiloso gera vantagem econômica no objeto da contratação a ser realizada, uma vez que o preço máximo estimado no procedimento não servirá como parâmetro para os participantes do procedimento licitatório, o que pode gerar economia para o ente público, bem como avaliará a participação de empresas com expertise e capacidade gerencial, inibindo, no futuro, eventual prejuízo na execução contratual. 9.4 O valor referencial obtido, em pesquisa de preços, para esta aquisição/serviço está muito superior ao praticado, atualmente, por esta Administração. Desta forma, o custo estimado da contratação possuirá caráter sigiloso e será tornado público em momento posterior à homologação.]

11. Adequação orçamentária

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do Estado.

11.2. No presente exercício, a contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: Gestão/Unidade: SEC. DA JUSTIÇA E CIDADANIA / FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO - 990202;

II) Fonte de Recursos: 1.500.1.0.001;

III) Programa de Trabalho: 04.122.1729.6551.0000;

IV) Elemento de Despesa: 3.3.90.40.90.

11.3. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

12. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

VANESSA VALENTE

Autoridade competente

Assinou eletronicamente em 20/05/2025 às 18:56:33.

A N E X O I.1

Item	Qtde	Especificação
		LISTA DE EQUIPAMENTOS – PARTE A
01	03	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 2 Discos de 300GB SAS Marca: Dell Modelo: Power Edge R630 Consulta: Localidade: Fundação Casa
02	01	Storage 12 discos SSD 1.92 TB Marca: Dell Modelo: ME4024 Consulta: https://www.delltechnologies.com/asset/en-us/products/storage/technical- support/h17384-powervault-me4-series-ss.pdf Localidade: Fundação Casa
03	02	Storage 12 discos 8 TB Marca: Dell Modelo: ME412 Consulta: https://www.delltechnologies.com/asset/en-us/products/storage/technical- support/h17384-powervault-me4-series-ss.pdf Localidade: Fundação Casa
04	01	Storage 12 discos NL-SAS 16 TB Marca: Dell Modelo: ME5012 Localidade: Fundação Casa
05	01	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 1 Disco de 1.2 TB SAS Marca: Dell Modelo: Power Edge R640 Localidade: Fundação Casa
06	03	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 1 Disco de 1.2TB SAS Marca: Dell Modelo: Power Edge R650 Localidade: Fundação Casa
07	01	Tape Library drivers LTO8 FC Marca: DELL Modelo: ML3 Localidade: Fundação Casa

		LISTA DE EQUIPAMENTOS – PARTE B
08	04	Switches 48 portas 10GbE Marca: Dell Modelo: S4820T Localidade: Fundação Casa
09	03	Servidores Rack com 2 Processadores Six Core, 128GB RAM e 2 Discos de 300GB SAS Marca: IBM Modelo: System x3850 X5 Serial Number: TR014MK, TR014MG, TR01492 Consulta: https://lenovopress.com/tips0817-system-x3850-x5 Localidade: Fundação Casa
10	01	Appliance de Monitoramento Localidade: Fundação Casa
11	01	Tape Library IBM 2 drivers LTO6 FC Marca: DELL Modelo: TL2000 Consulta: https://i.dell.com/sites/csdocuments/Shared-Content_data- Sheets_Documents/pt/br/ss676-powervault-tl2000-tape-library_br.pdf Localidade: Fundação Casa
		LISTA DE SOFTWARES – PARTE C
12	02	VMWare vSphere Essentials Plus Kit 6 Marca: VMware Produto: vSphere Essentials Plus Kit Consulta: https://www.vmware.com/files/br/pdf/vsphere/VMware-vSphere-Essentials- Editions-Datasheet.pdf Localidade: Fundação Casa
13	02	Solução de Segurança Marca: Fortinet Modelo: Fortigate 1101E Licenciamento: UTP Consulta: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf Localidade: Fundação Casa

Estudo Técnico Preliminar 46/2025

1. Informações Básicas

Número do processo: 161.00039823/2025-01

2. Descrição da necessidade

2.1 Contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes.

2.2 A contratação busca garantir a segurança, a integridade e a alta disponibilidade dos dados e serviços hospedados no Datacenter da Instituição já disponibilizados e em pleno funcionamento, garantindo uma rápida recuperação operacional dos serviços em caso de falhas físicas e lógicas através de manutenções corretivas e preventivas. Além de garantir a continuidade de atualização dos softwares, firmwares e patches de segurança para as mais recentes versões, além de licenças para garantir o funcionamento de serviços críticos nas plataformas de segurança.

3. Área requisitante

Área Requisitante	Responsável
ATI - Assessoria de Tecnologia da Informação	Leandro Timossi de Almeida

4. Necessidades de Negócio

Conforme justificado no item 2 (Descrição da Necessidade), faz-se necessária a contratação de uma solução que ofereça serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes, para que a Fundação CASA-SP não tenha seus serviços e operação tecnológica comprometida.

Outra necessidade crítica é a manutenção do licenciamento dos serviços de segurança do Firewall de próxima geração em funcionamento. Recurso indispensável para manter o ambiente computacional seguro, pois essa ferramenta é responsável por monitorar todo o tráfego que entra e sai da rede, inspecionando os pacotes e protegendo contra ameaças cibernéticas modernas. Sem tal recurso nossa estrutura estará severamente vulnerável.

A presente demanda trata em parte da renovação das licenças dos serviços do Firewall de Próxima Geração (NGFW) da Fundação CASA-SP (pois manter o licenciamento desse equipamento ativo, garante que a ferramenta mantenha-se atualizada e capaz de impedir que novas ameaças possam comprometer a integridade e disponibilidade da rede) e também da manutenção dos equipamentos do Data Center da Fundação CASA-SP.

Quanto ao Datacenter, vários equipamentos de alta criticidade, como servidores, storages e outros equipamentos que integram o core do ambiente e que possuíam garantia da fabricante, estão com

as garantias próximas do vencimento, exigindo a inclusão dessas soluções em um contrato de manutenção.

Em virtude da criticidade desses equipamentos, possíveis falhas podem resultar em paradas de serviços críticos, resultando em indisponibilidade de sistemas, falhas no acesso a estrutura de dados corporativos usados diariamente em toda a organização, entre outros.

Diante do cenário exposto, com as necessidades do negócio estabelecidas, em virtude da complexidade do ambiente e da criticidade das aplicações existentes e em produção, para garantir a integridade e disponibilidade da estrutura computacional da Fundação CASA-SP e também garantir melhor gestão decidiu-se por centralizar a contratação dos serviços acima descritos e também permitir maior perenidade à estrutura computacional, já que dessa forma será possível manter o ambiente atualizado e com a estrutura protegida contra possíveis descontinuidades decorrentes de expiração de prazos de vigências para serviços tais, como fim de garantias e renovação de licenças, indispensáveis para o correto funcionamento de toda a estrutura.

Considerando a imprescindibilidade dos serviços e os requisitos da contratação, deve ser exigida, dos licitantes, a comprovação de que possuem qualificação econômico-financeira e qualificação técnica, com elementos que garantam o efetivo cumprimento das obrigações contratuais e a mitigação de riscos quanto à interrupção dos serviços.

Qualificação econômico-financeira:

Comprovação de que a empresa licitante não se encontra em processo falimentar.

Comprovação de que o licitante possui aptidão econômica licitante para cumprir as obrigações decorrentes do futuro contrato, através da exigência de documentação que evidencie o atendimento aos coeficientes e índices econômicos usualmente empregados no mercado.

Qualificação técnica:

Comprovação de que o licitante possui capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior aos serviços a serem contratados, mediante a apresentação de atestados de capacidade técnica, que demonstrem, ao menos os seguintes elementos:

> a) Deverá haver a comprovação da experiência mínima de 01 (um) ano na prestação de serviços similares, sendo aceito o somatório de atestados ou certidões de períodos diferentes, não havendo obrigatoriedade de os anos serem ininterruptos.

5. Necessidades Tecnológicas

5.1 Os itens a serem contratados serão licitados em apenas uma solução, prestados por uma única empresa visando a racionalização e gestão com ampla definição de responsabilidade em caso de acionamento da garantia, tendo em vista que todo o sistema tem grande complexidade, evitando-se comprometer a efetividade do serviço prestado.

5.2 Em virtude da complexidade do ambiente e da criticidade das aplicações existentes e em produção, os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte A deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

5.3 Os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte B poderão ser prestados diretamente pelo próprio fabricante correlacionado ao produto (Dell, IBM, HP, Fortinet, etc.) ou por seus parceiros autorizados.

5.4 Os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware e Fortigate listados na tabela – parte C deverão ser prestados pelo próprio fabricante (Vmware e Fortinet) para todas as licenças existentes na Fundação Casa.

5.5 A fim de manter a qualidade dos serviços prestados para a Fundação Casa, caso haja a necessidade a CONTRATANTE poderá solicitar a substituição de qualquer equipamento listado na tabela - parte A, por um equipamento novo desde que se encontre em linha de produção e sem uso anterior devidamente aprovado pela equipe técnica da Fundação Casa. Este equipamento deverá ter performance igual ou superior ao já existente e deverá possuir garantia direta pelo fabricante do produto.

5.6 Em virtude da grande complexidade técnica do ambiente em produção na Fundação Casa, por se tratar de um ambiente em produção com aplicações críticas, bem como a fim de garantir a competência técnica da licitante que prestará os serviços objeto deste contrato, a licitante deverá apresentar as seguintes declarações para fins de habilitação:

5.6.1 Declaração, firmada por representante legal da licitante, sob as penas da lei, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que possui em seu quadro de colaboradores, no mínimo, 02 (dois) profissionais técnicos certificados pelo fabricante Dell nas áreas de servidores, storage e redes (network), além de 1 (um) profissional técnico certificado pelo fabricante Fortinet nas áreas de firewall.

5.6.2 Declaração, firmada por representante legal da licitante, sob as penas da lei, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia e assistência técnica para os equipamentos listados na tabela – parte A, deverão ser prestados diretamente e exclusivamente pelo fabricante dos equipamentos Dell.

5.6.3 Declaração, firmada por representante legal da licitante, sob as penas da lei, comprometendo-se a apresentar, por ocasião da celebração do contrato, comprovação de que os serviços de garantia, suporte técnico e atualização tecnológica para as licenças de software Vmware listados na tabela – parte C serão prestados pelo próprio fabricante (Vmware e Fortinet), para todas as licenças existentes na Fundação CASA-SP.

5.7 A CONTRATADA deverá ofertar recursos em nuvem com capacidade para oferecer a estrutura mínima para que a Fundação CASA-SP seja capaz de executar uma recuperação de desastre em ambiente virtualizado, oferecendo recursos para backup e proteção, a fim de garantir a continuidade dos serviços críticos essenciais, conforme descrição e recursos a serem apresentados no termo de referência.

5.8 A instalação e configuração dos serviços sempre deverá ser realizada de acordo com as melhores práticas recomendadas pelos fabricantes, de forma a alcançar a funcionalidade esperada e o nível de segurança ideal. Desta forma também é importante que as equipes envolvidas com os serviços contratados possuam a qualificação necessária e capacidade técnica e fim de resolver qualquer demanda futura.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1 Em decorrência da criticidade do ambiente computacional da Fundação CASA-SP, A CONTRATADA deverá oferecer suporte técnico pelo período 24x7, por 365 dias, para manutenção preventiva e/ou corretiva, além de suporte para a equipe da CONTRATANTE, oferecendo recursos para abertura de chamado seja por telefone ou via plataforma online.

6.2 A CONTRATADA também deverá ser capaz de manter o monitoramento do ambiente computacional da Fundação CASA-SP, por meio de recursos físicos ou online, de forma a permitir intervenções necessárias em decorrência de falhas ou maus funcionamentos dos equipamentos que compõem a estrutura coberta pelo contrato.

6.2 A CONTRATADA deverá garantir que todas as operações de manutenção do datacenter estejam em conformidade com normas e regulamentações locais, como a LGPD (Lei Geral de Proteção de Dados), ISO 27001, entre outras.

6.3 A CONTRATADA deverá garantir que os serviços prestados atendam os seguintes requisitos:

- Alta Disponibilidade: O serviço de manutenção deve garantir um nível máximo de uptime, minimizando as interrupções no serviço do datacenter, atendendo a SLA a ser detalhada no termo de referência.
- Segurança: Garantir que todas as manutenções e atividades no datacenter sejam realizadas seguindo práticas de segurança da informação e protocolos de confidencialidade, comprometendo-se a atender as legislações vigentes.
- Eficiência Operacional: Buscar maximizar a eficiência dos recursos do datacenter, garantindo o uso otimizado da infraestrutura e reduzindo custos operacionais sem comprometer a qualidade dos serviços entregues pelo Datacenter.

6.4 Justificativa para o Parcelamento ou não da Solução

6.4.1. A proposta abrange a contratação de apenas 01 solução capaz de entregar de forma integral todo o licenciamento e a manutenção do núcleo principal da infraestrutura computacional da Fundação CASA-SP. O parcelamento do objeto compromete a gestão, o monitoramento e todo o processo de suporte, pois dois ou mais contratos do mesmo objeto aumentaria a complexidade de gerenciamento do ambiente, o que poderia resultar em possíveis falhas e a não cobertura completa para os equipamentos envolvidos.

6.4.2. Sobre o princípio do parcelamento, destaca-se, que a alínea “b” do inciso V do art. 40 da Lei 14.133 estabelece que este princípio deve ser atendido quando a contratação for tecnicamente e economicamente viável. Além disso, é importante esclarecer que o § 3º do mesmo artigo orienta que o parcelamento não será adotado quando:

“I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.”

6.4.3. O fracionamento da contratação com o objetivo de aplicar cotas de participação exclusiva para microempresas e empresas de pequeno porte comprometeria a gestão eficiente da solução de TI, além de reduzir os benefícios da economia de escala esperados. Essa fragmentação

não se mostra vantajosa para a Administração Pública e poderia resultar em prejuízos à execução adequada do objeto contratado. Dessa forma, esta comissão de contratação considera inviável o parcelamento deste objeto, sendo essencial que sua execução ocorra de forma integral por uma única empresa contratada.

6.5 Habilitações jurídicas

6.5.1 Quanto a participação de consórcios e cooperativas:

Consórcios: Não há elementos que indiquem qualquer prejuízo ao cumprimento das obrigações contratuais em caso de formação de consórcios para a participação na licitação, dentro dos limites da lei.

De igual modo, não há nenhuma demanda para que se exija percentuais específicos a serem considerados para as condições de qualificação econômico-financeira. Dessa forma, deve ser observado o percentual mínimo de 10% (dez por cento), na forma do art. 15, §1º da Lei Federal nº 14.133/2021.

Participação de Cooperativas: Podem participar da licitação pública, desde que cumpram as condições estabelecidas na Lei nº 14.133/2021.

6.6. Não haverá exigência de garantia da contratação disposta no art. 96 e seguintes da Lei nº 14.133/2021.

7. Estimativa da demanda - quantidade de bens e serviços

Os quantitativos dos produtos discriminados na tabela a seguir foram estimados a partir das necessidades de manutenção do Datacenter, considerando a atual estrutura, com a intenção de manter o ambiente protegido e disponível em virtude da criticidade dos serviços.

Item	Qtde	Especificação
		LISTA DE EQUIPAMENTOS – PARTE A
01	03	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 2 Discos de 300GB SAS Marca: Dell Modelo: Power Edge R630 Consulta: Localidade: Fundação Casa
02	01	Storage 12 discos SSD 1.92 TB Marca: Dell Modelo: ME4024 Consulta: https://www.delltechnologies.com/asset/en-us/products/storage/technical-support/h17384-powervault-me4-series-ss.pdf

		Localidade: Fundação Casa
03	02	Storage 12 discos 8 TB Marca: Dell Modelo: ME412 Consulta: https://www.delltechnologies.com/asset/en-us/products/storage/technical-support/h17384-powervault-me4-series-ss.pdf Localidade: Fundação Casa
04	01	Storage 12 discos NL-SAS 16 TB Marca: Dell Modelo: ME5012 Localidade: Fundação Casa
05	01	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 1 Disco de 1.2 TB SAS Marca: Dell Modelo: Power Edge R640 Localidade: Fundação Casa
06	01	Servidores Rack com 2 Processadores Octa Core, 256GB RAM e 1 Disco de 1.2TB SAS Marca: Dell Modelo: Power Edge R650 Localidade: Fundação Casa
07	01	Tape Library drivers LTO8 FC Marca: DELL Modelo: ML3 Localidade: Fundação Casa
		LISTA DE EQUIPAMENTOS – PARTE B
08	04	Switches 48 portas 10GbE Marca: Dell Modelo: S4820T Localidade: Fundação Casa

09	03	Servidores Rack com 2 Processadores Six Core, 128GB RAM e 2 Discos de 300GB SAS Marca: IBM Modelo: System x3850 X5 Serial Number: TR014MK, TR014MG, TR01492 Consulta: https://lenovopress.com/tips0817-system-x3850-x5 Localidade: Fundação Casa
10	01	Appliance de Monitoramento Localidade: Fundação Casa
11	01	Tape Library IBM 2 drivers LTO6 FC Marca: DELL Modelo: TL2000 Consulta: https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/pt/br/ss676-powervault-tl2000-tape-library_br.pdf Localidade: Fundação Casa
		LISTA DE SOFTWARES – PARTE C
12	02	VMWare vSphere Essentials Plus Kit 6 Marca: VMware Produto: vSphere Essentials Plus Kit Consulta: https://www.vmware.com/files/br/pdf/vsphere/VMware-vSphere-Essentials-Editions-Datasheet.pdf Localidade: Fundação Casa
13	02	Solução de Segurança Marca: Fortinet Modelo: Fortigate 1101E Licenciamento: UTP Consulta: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf Localidade: Fundação Casa

8. Levantamento de soluções

Foram consideradas as possíveis soluções para atendimento da atual demanda, com capacidade para pleno atendimento das necessidades da instituição:

Id	Descrição da solução (ou cenário)
1	Renovação de Garantia de Hardware e Softwares através de fornecedores, com manutenção preventiva e corretiva
2	Aquisição de nova solução de hardware e software
3	Aquisição de nova solução em nuvem

9. Análise comparativa de soluções

ANÁLISE COMPARATIVA DE SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	Renovação de Garantia de Hardware e Softwares através de fornecedores, com manutenção preventiva e corretiva
2	Aquisição de nova solução de hardware e software
3	Aquisição de nova solução em nuvem

A comparação entre renovação e aquisição envolve uma série de considerações, incluindo desempenho, custo, segurança, escalabilidade e complexidade de gerenciamento. Abaixo, vamos destacar os principais pontos de comparação entre os dois:

1. Desempenho:

Renovação de Garantia: O desempenho e os recursos atuais se manteriam atendendo a demanda e a carga de trabalho atual.

Servidores Físicos: Geralmente oferecem desempenho previsível e consistente, pois os recursos são dedicados exclusivamente à carga de trabalho.

Nuvem: O desempenho pode variar dependendo da demanda do provedor de nuvem e do compartilhamento de recursos. No entanto, muitos provedores de nuvem oferecem opções de instâncias de alta performance para atender às necessidades exigentes de algumas cargas de trabalho.

2. Custos:

Renovação de Garantia: A renovação de garantia pode ser uma opção mais econômica a curto prazo, pois você está estendendo a vida útil do equipamento existente sem grandes desembolsos contínuos.

Servidores Físicos: Exigem investimento inicial significativo em hardware, além de custos contínuos de manutenção, energia elétrica, refrigeração e espaço físico.

Nuvem: Normalmente opera sob um modelo de pagamento conforme o uso, o que pode ser mais econômico para empresas que têm cargas de trabalho variáveis ou precisam escalar rapidamente.

3. Segurança:

Renovação de Garantia: A renovação de garantia dos hardwares e softwares permitem a continuidade das atualizações de segurança e funcionalidades.

Servidores Físicos: Oferecem controle direto sobre a segurança, mas exigem a implementação e manutenção de medidas de segurança física e lógica.

Nuvem: Muitos provedores de nuvem possuem certificações de segurança e oferecem uma variedade de recursos de segurança, incluindo firewalls, criptografia e gerenciamento de identidade. No entanto, a segurança dos dados na nuvem depende da confiança no provedor de serviços e da implementação correta de medidas de segurança por parte do usuário.

4. Escalabilidade:

Renovação de Garantia: A escalabilidade se mantem limitada com o hardware atual e disponível.

Servidores Físicos: A escalabilidade pode ser limitada pela capacidade de hardware disponível e pelo tempo necessário para adquirir e configurar novos servidores.

Nuvem: Oferece escalabilidade quase instantânea, permitindo aumentar ou diminuir os recursos conforme necessário, pagando apenas pelo que é usado.

5. Complexidade de Gerenciamento:

Renovação de Garantia: A estrutura atual já possui os recursos de gerenciamento em produção, não necessitando de ajustes extras.

Servidores Físicos: Exigem gerenciamento direto de hardware, atualizações de software e configuração de rede, o que pode ser complexo e exigir habilidades especializadas.

Nuvem: Geralmente oferece ferramentas de gerenciamento centralizado que simplificam muitas tarefas administrativas, mas ainda requerem conhecimento técnico para configurar e otimizar adequadamente.

6. Confiabilidade e Disponibilidade:

Renovação de Garantia: Evita interrupções na operação devido a falhas não cobertas pela garantia, pois você mantém o suporte do fabricante.

Servidores Físicos: A disponibilidade depende da redundância e da qualidade do hardware e infraestrutura de rede.

Nuvem: Muitos provedores de nuvem oferecem SLAs (Acordos de Nível de Serviço) que garantem alta disponibilidade e podem oferecer recursos de redundância geográfica para aumentar a confiabilidade.

7. Flexibilidade:

Renovação de Garantia: A flexibilidade se mantem limitada com o hardware atual e disponível.

Servidores Físicos: Oferecem total controle sobre o hardware e o software, permitindo customização completa de acordo com as necessidades da empresa.

Nuvem: Oferece uma ampla gama de serviços e recursos, permitindo que as empresas escolham entre várias opções de configuração e migrem entre elas conforme necessário.

Em resumo, a escolha entre nuvem e servidores físicos depende das necessidades específicas de cada empresa, incluindo requisitos de desempenho, custo, segurança e flexibilidade. Muitas empresas optam por uma abordagem híbrida, combinando servidores físicos para cargas de trabalho específicas com a utilização de serviços de nuvem para flexibilidade e escalabilidade.

1 Renovação de Garantia:

Vantagens:

1. Proteção contra Custos Inesperados: A renovação da garantia pode proteger contra custos inesperados de reparo ou substituição de hardware em caso de falha. Isso pode ajudar a prever e gerenciar melhor os custos operacionais.
2. Continuidade Operacional: Ao manter a garantia, a empresa garante acesso ao suporte técnico do fabricante, o que pode ser crucial para minimizar o tempo de inatividade em caso de problemas.
3. Manutenção de Ativos Existentes: Se os equipamentos ainda atendem às necessidades da empresa em termos de desempenho e capacidade, renovar a garantia pode ser uma maneira econômica de prolongar sua vida útil e maximizar o retorno sobre o investimento inicial.
4. Conformidade com Contratos e Acordos de Nível de Serviço (SLAs): Em muitos casos, a renovação da garantia pode ser necessária para cumprir os requisitos contratuais ou SLAs com clientes ou parceiros.

Desvantagens:

1. Custo: A renovação da garantia pode representar um custo significativo, especialmente se a empresa tiver muitos equipamentos que precisam ser cobertos. Esse custo pode ser percebido como desnecessário se os equipamentos estiverem funcionando bem e não houver histórico de falhas.
2. Obsolescência Tecnológica: Mesmo que a garantia seja renovada, os equipamentos ainda podem se tornar obsoletos em termos de tecnologia, desempenho ou recursos em comparação com as opções mais recentes disponíveis no mercado.
3. Limitações de Cobertura: Nem todos os problemas podem ser cobertos pela garantia, e pode haver cláusulas ou exclusões que restringem a cobertura para certos tipos de danos ou condições de uso.
4. Flexibilidade Limitada: Renovar a garantia pode prender a empresa a uma determinada marca ou modelo de hardware por um período adicional de tempo, reduzindo a flexibilidade para adotar novas tecnologias ou fornecedores.

Servidores Físicos:

Vantagens:

5. Controle total: Os servidores físicos oferecem controle total sobre hardware e software, permitindo ajustes precisos de configuração.
6. Desempenho previsível: Com recursos dedicados, os servidores físicos geralmente oferecem desempenho mais previsível e consistente.
7. Segurança: Alguns argumentam que os servidores físicos oferecem maior controle e segurança sobre os dados, pois estão diretamente sob o controle da organização.
8. Custos previsíveis a longo prazo: Enquanto os custos iniciais de investimento podem ser mais altos, a manutenção de servidores físicos pode ser mais previsível ao longo do tempo, sem taxas mensais.

Desvantagens:

5. Custos iniciais elevados: Aquisição de hardware, instalação e configuração podem resultar em custos iniciais significativos.
6. Manutenção e atualização: As empresas são responsáveis pela manutenção, atualização e substituição de hardware e software, o que pode exigir tempo e recursos significativos.
7. Escalabilidade limitada: A capacidade de escalabilidade é limitada pela capacidade física do hardware existente, o que pode resultar em problemas de capacidade em momentos de crescimento rápido ou inesperado.
8. Riscos de tempo de inatividade: Falhas de hardware podem resultar em tempo de inatividade significativo, especialmente se não houver medidas de redundância adequadas.

Nuvem:

Vantagens:

1. Escalabilidade: Os serviços em nuvem oferecem escalabilidade instantânea, permitindo que as empresas aumentem ou diminuam os recursos conforme necessário.
2. Redução de custos iniciais: As soluções em nuvem geralmente envolvem custos operacionais mensais ou anuais, em vez de grandes investimentos iniciais em hardware.

3. Manutenção simplificada: A manutenção de hardware e software é de responsabilidade do provedor de nuvem, liberando a equipe de TI interna para se concentrar em outras áreas.
4. Disponibilidade e redundância: Muitos provedores de nuvem oferecem redundância geográfica e recursos de alta disponibilidade, reduzindo significativamente o risco de tempo de inatividade.

Desvantagens:

1. Dependência de conexão com a internet: Acesso aos recursos em nuvem depende de uma conexão estável com a internet. Interrupções na conectividade podem resultar em indisponibilidade temporária.
2. Segurança percebida: Alguns podem ter preocupações sobre a segurança dos dados na nuvem, embora os provedores de nuvem geralmente implementem medidas rigorosas de segurança, mas que exigem equipes qualificadas para que a configuração do ambiente seja realizada de forma adequada, a fim de garantir a proteção do ambiente.
3. Custos variáveis: Enquanto os custos iniciais podem ser menores, os custos operacionais contínuos podem variar dependendo do uso e da demanda.
4. Personalização limitada: Em alguns casos, a personalização de configurações de hardware ou software pode ser limitada em comparação com servidores físicos.

Pesquisa de Produtos

Exploramos várias opções de equipamentos, softwares e soluções de diferentes fabricantes através de sugestões de parceiros, fornecedores e informações públicas dos catálogos dos produtos acessíveis na internet em sites oficiais, incluindo Dell, HP, e Lenovo, Veeam, Veritas, etc.

Avaliação de Opções para aquisição (Servidores)

Após análise detalhada, identificamos os seguintes modelos como candidatos promissores:

- Dell PowerEdge
- HP ProLiant
- Lenovo ThinkSystem
- Supermicro

Avaliação de Opções para aquisição (Storage)

Após análise detalhada, identificamos os seguintes modelos como candidatos promissores:

- Dell PowerVault ME5024
- HP MSA 2060
- Lenovo ThinkSystem DM3000H
- PureStorage FlashArray

Avaliação de Opções para aquisição (Switches)

Após análise detalhada, identificamos os seguintes modelos como candidatos promissores:

- Dell Networking PowerSwitch
- Cisco
- HPE Aruba
- Huawei

Avaliação de Opções para aquisição (Solução de Backup)

Após análise detalhada, identificamos os seguintes modelos como candidatos promissores:

- Veeam
- Dell PowerProtect
- Veritas Netbackup

Avaliação de Opções para ambiente alocado em nuvem

Após análise detalhada, identificamos os seguintes modelos como candidatos promissores:

- Azure
- AWS
- Equinix
- Uol host

10. Registro de soluções consideradas inviáveis

Durante o processo de avaliação e seleção de infraestrutura de TI para a Instituição, consideramos diversas opções, incluindo a adoção de servidores em nuvem. No entanto, após análise cuidadosa, identificamos várias razões pelas quais essas soluções foram consideradas inviáveis:

1. **Dependência de Conectividade com a Internet:**
    - Reconhecemos que a disponibilidade e o desempenho dos serviços em nuvem estão diretamente ligados à qualidade e disponibilidade da conexão com a internet. Em áreas com conectividade limitada ou instável, isso pode representar um risco significativo para as operações da empresa.
2. **Custos Operacionais Variáveis:**
    - Embora os custos iniciais possam ser mais baixos, a natureza variável dos custos operacionais em nuvem pode tornar a previsão financeira mais desafiadora a longo prazo. Variações no uso e na demanda podem resultar em faturas imprevisíveis, o que pode afetar o planejamento financeiro da organização.
3. **Segurança Percebida:**
    - Apesar dos avanços em segurança na nuvem, algumas preocupações persistentes sobre a segurança dos dados na nuvem ainda existem. Para dados altamente sensíveis ou regulamentados, como informações dos adolescentes atendidos pela Fundação, dados pessoais, financeiras ou de saúde, a percepção de risco pode ser um obstáculo significativo para a adoção da nuvem.
4. **Personalização Limitada:**

- Em alguns casos, as opções de personalização de infraestrutura em nuvem podem ser limitadas em comparação com servidores físicos. Isso pode restringir a capacidade da empresa de adaptar a infraestrutura às suas necessidades específicas, levando a compromissos no desempenho ou na funcionalidade.

5. **Necessidades Específicas de Desempenho ou Conformidade:**

- Para cargas de trabalho que exigem desempenho previsível ou que estão sujeitas a requisitos regulatórios específicos, como conformidade com a Lei Geral de Proteção de Dados (LGPD) no Brasil, a nuvem pode não oferecer os níveis necessários de controle ou conformidade.

11. Análise comparativa de custos (TCO)

11.1 Os custos totais de propriedade são apresentados e comparados a seguir:

Solução Viável 1
Descrição:
Suporte técnico e garantia onsite para equipamentos e infraestrutura de sustentação.
Custo Total de Propriedade – Memória de Cálculo
R$ 98.374,00 (Mensal)
Solução Viável 2
Descrição:
Ambiente on-premisse com a aquisição de novos recursos computacionais armazenamento e segurança.
Custo Total de Propriedade – Memória de Cálculo
R$ 4.097.500,00 (Parcela única)
Solução Viável 3
Descrição:
Solução de ambiente em nuvem e armazenamento em nuvem.

Custo Total de Propriedade – Memória de Cálculo
R$ 5.160.000,00

11.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

De posse dos preços levantados, realizou-se uma análise crítica sobre os valores, a fim de verificar se dentre eles havia sobrepreços ou preços inexequíveis.

Descrição da solução	Estimativa de TCO ao longo dos 3 anos			Total
	Ano 1	Ano 2	Ano 3	
Solução Viável 1	R$ 1.180.488,00	R$ 1.180.488,00	R$ 1.180.488,00	R$ 3.541.464,00
Solução Viável 2	R$ 3.627.500,00	R$ 235.000,00	R$ 235.000,00	R$ 4.097.500,00
Solução Viável 3	R$ 1.720.000,00	R$ 1.720.000,00	R$ 1.720.000,00	R$ 5.160.000,00

12. Descrição da solução de TIC a ser contratada

A Renovação de Garantia de Hardware e Softwares através de fornecedores, com manutenção preventiva e corretiva do Datacenter irá proporcionar um ambiente totalmente licenciado e com suporte pelos próximos anos. Esse renovação do suporte do ambiente irá permitir uma maior agilidade na gestão do ambiente em caso de problemas técnicos, aumento da eficiência dos recursos de hardware utilizados, utilização de novas tecnologias atualizadas para aumentar a segurança dos dados da Instituição e prover a capacidade da equipe de Infraestrutura de TI de se adaptar a novas demandas.

13. Estimativa de custo total da contratação

[Conteúdo Sigiloso | Justificativa: O sigilo tem por finalidade garantir a melhor oferta para a contratação.]

14. Justificativa técnica da escolha da solução

As justificativas técnicas para a solução escolhida foram baseadas na análise de fatores como a desempenho, segurança, conformidade, integridade da estrutura e continuidade da operação. Conforme já apontada entre as vantagens da solução escolhida destacamos que ela oferecerá ao órgão proteção contra custos inesperados, pois em caso de falhas no ambiente decorrentes de problemas em equipamentos, a troca do equipamento com problema está garantida.

Equipamentos de alta performance costumam ter custos, cuja aquisição podem resultar em demora devido a necessidade de realização de pregões eletrônicos ou do próprio processo de compra como um todo, comprometendo a recuperação do ambiente e a regularização dos serviços. Fato que corrobora outro fator levado em consideração, que é a continuidade operacional da estrutura computacional da Fundação CASA-SP. Com a renovação da garantia, o suporte técnico é realizado pelo fabricante, minimizando problemas de incompatibilidade de componentes, ou que estejam em desacordo com os equipamentos em operação.

A opção da renovação a ainda garante que serviços críticos não necessitem de novas implementações e reconfigurações no ambiente, que devido a complexidade podem resultar em possíveis falhas e paradas em serviços críticos, comprometendo significativamente as atividades diárias da organização. Novas implementações, substituições de equipamentos obrigam a um planejamento bastante acurado, que exigem janelas para execução de atividades de substituição e configuração dos equipamentos, etc.

15. Justificativa econômica da escolha da solução

As justificativas para a decisão foram baseadas na análise das necessidades, recursos, custos e riscos específicos.

Para a administração pública, além das várias razões técnicas, já apontadas, pelas quais a solução a ser contratada pela Fundação CAS-SP, considerou-se também a vantajosidade econômica conforme a seguinte justificativa:

Custos: Os custos para manter os serviços técnicos especializados no datacenter da Fundação CASA-SP serão pagos mensalmente, que simplifica os planejamentos orçamentários e financeiros. Além disso, a administração deixa de realizar um investimento inicial alto para construção de um datacenter ou na aquisição de novos equipamentos por um certo período, cujo valor de investimento inicial é bastante considerável, e que num período relativamente curto de tempo pode ficar defasado.

Em comparação as demais soluções, no curto e médio prazo os valores apresentados ainda são vantajosos para a instituição. Os benefícios decorrentes da contratação justificam os custos envolvidos.

16. Benefícios a serem alcançados com a contratação

A contratação da solução selecionada possibilitará uma série de benefícios, destacando-se os seguintes:

16.1. Continuidade e Estabilidade Operacional

- **Benefício**: A solução escolhida garantirá a continuidade dos serviços essenciais de operação e manutenção do datacenter, evitando interrupções no fornecimento de serviços críticos.

16.2. Redução de Riscos e Custos de Transição

- **Benefício**: A renovação de contratos evita a necessidade de um novo processo licitatório e os custos associados a uma nova transição, como treinamento de equipes, adaptação a novos fornecedores e ajustes nos sistemas existentes. A própria lei 14.133/21 prevê a possibilidade de renovação contratual de forma a evitar a instabilidade gerada por mudanças constantes de fornecedores, especialmente em contratos técnicos especializados, como os de manutenção de datacenters, o que corresponde ao atual cenário.

16.3. Aprimoramento da Qualidade do Serviço

- **Benefício**: Com a solução selecionada, o fornecedor já estará ciente das especificidades do datacenter, o que possibilitará um serviço de manutenção mais especializado e com maior nível de qualidade, maior eficiência e eficácia no atendimento das demandas críticas.

16.4. Maior Previsibilidade e Planejamento Orçamentário

- **Benefício**: A solução escolhida permite maior previsibilidade de custos e facilita o planejamento orçamentário, já que os valores e as condições para manutenção serão mantidos, ou ajustados de forma transparente, ao longo do tempo.

16.5. Garantia de Conformidade Regulatória e Tecnológica

- **Benefício**: Ao contratar a solução escolhida com um fornecedor experiente, garante-se que os serviços de manutenção atendam às exigências legais, regulatórias e de segurança, mantendo o ambiente atualizado com as melhores práticas e normas do setor.

16.6. Melhoria no Relacionamento com o Fornecedor

- **Benefício**: A solução escolhida contribuirá para estabelecer um relacionamento de longo prazo com o fornecedor, promovendo a confiança mútua e a resolução mais eficiente de problemas, além de possibilitar melhorias contínuas no serviço prestado.

16.7. Garantia de Suporte Técnico Especializado

- **Benefício**: A solução escolhida garantirá também que a equipe de manutenção já conheça profundamente as especificidades técnicas do datacenter, resultando em um suporte mais ágil e eficiente.

17. Providências a serem Adotadas

Não há necessidade de adequação do ambiente para a utilização dos produtos objetos desta contratação. Trata-se de produtos já conhecidos pela equipe de administração da infraestrutura da Fundação CASA-SP, assim não haverá necessidade de nenhum treinamento e nem preparação prévia. A Fundação CASA-SP já possui a mão de obra especializada para manutenção da estrutura existente e que será mantida na modalidade escolhida.
Esta renovação das licenças e garantias deverá garantir a continuidade dos serviços ativos, sejam de segurança ou da proteção da infraestrutura com um todo.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A solução escolhida se justifica pela necessidade de uma solução com recursos computacionais visando a entrega de novos serviços e segurança, pois eles serão essenciais para a realização das operações diárias da instituição mantendo a sua integridade e acessibilidade. Sem essa solução, as operações da empresa podem ser severamente impactadas, levando a interrupções no serviço, perda de informações e atrasos no trabalho e perda de produtividade.

Investir nesta solução permite que a empresa se mantenha atualizada com as últimas tecnologias, melhorando o desempenho, segurança e confiabilidade das operações de TI.

A justificativa para esta escolha baseia-se na disponibilidade orçamentaria para custeio da aquisição.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ODENILSON DOS SANTOS BONFIM

Equipe de Planejamento

Assinou eletronicamente em 19/05/2025 às 15:06:50.

LEANDRO TIMOSSI DE ALMEIDA

Equipe de Planejamento

Assinou eletronicamente em 19/05/2025 às 15:08:25.

ANEXO II

MINUTA DE TERMO DE CONTRATO

FUNDAÇÃO CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE - FUNDAÇÃO CASA-SP

Processo Administrativo SEI n°.....

Pregão Eletrônico n°.....

Contrato ___ n°.....

Código Único: n°.....

CONTRATO ADMINISTRATIVO Nº ...../...., CELEBRADO ENTRE A FUNDAÇÃO CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE – FUNDAÇÃO CASA ....., POR INTERMÉDIO DO(A) ..... E .....

A FUNDAÇÃO CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE - FUNDAÇÃO CASA-SP, instituída pela Lei n.º 185, de 12 de dezembro de 1973, com respectivas alterações, inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda sob o n.º 44.480.283/0001-91, sediada na Rua Florêncio de Abreu, n.º 848 – Luz - São Paulo - Capital, neste ato representada por sua Presidente, Ana Claudia Carletto, nos termos do Decreto de 03-05-2024, publicado no DOE de 06-05-2024 e por Vanessa Valente, Diretor Administrativo, nomeada nos termos da Portaria Administrativa n.º 1363/2024, no uso da competência conferida pela legislação aplicável, doravante denominado(a) CONTRATANTE, e o(a) ....., inscrito(a) no CNPJ/MF sob o nº ....., sediado(a) na ....., doravante designado(a) CONTRATADO, neste ato representado(a) por ..... (nome e função no contratado), inscrito(a) no CPF sob o nº....., conforme atos constitutivos da fornecedora OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº ..... e em

observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais normas da legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n. .../..., mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do Datacenter, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes, conforme detalhamento e especificações técnicas deste instrumento, do Termo de Referência, da proposta do Contratado e demais documentos da contratação constantes do processo administrativo em epígrafe.

1.2. O presente Termo de Contrato vincula-se à seguinte documentação, que se considera parte integrante deste instrumento, independentemente de transcrição:

1.2.1. O Termo de Referência;

1.2.2. O Edital da Licitação;

1.2.3. A Proposta do contratado; e

1.2.4. Eventuais anexos dos documentos supracitados.

1.3. O regime de execução deste contrato é o de empreitada por preço global.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses, contados da data estabelecida para início dos serviços, prorrogável por até 10 anos, a critério do Contratante, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. O Contratado poderá se opor à prorrogação de que trata o subitem acima, desde que o faça mediante documento escrito, recepcionado pelo Contratante em até 90 (noventa) dias antes do vencimento do contrato ou de cada uma das prorrogações do prazo de vigência.

2.1.2. Dentre outras exigências, a prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração e em harmonia com os preços do mercado, conforme pesquisa a ser realizada à época do aditamento pretendido, permitida a negociação com o Contratado, observando-se, ainda, os seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do Contratado informando o interesse na prorrogação;

e) Seja comprovado que o Contratado mantém as condições iniciais de habilitação.

2.1.3. O Contratado não tem direito subjetivo à prorrogação contratual, e não poderá pleitear qualquer espécie de indenização em razão da não prorrogação do prazo de vigência contratual por conveniência do Contratante.

2.1.4. Eventuais prorrogações de contrato serão formalizadas mediante celebração de termo aditivo, respeitadas as condições prescritas na Lei nº 14.133, de 2021.

2.1.5. Nas eventuais prorrogações contratuais, custos não renováveis já pagos ou amortizados no âmbito da contratação, quando houver, deverão ser eliminados como condição para a prorrogação.

2.1.6. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

2.1.7. Não obstante o prazo estipulado nesta cláusula, a vigência nos exercícios subsequentes ao da celebração do contrato estará sujeita a condições resolutivas consubstanciadas:

I - na inexistência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas, acarretando a extinção do contrato a partir de sua ocorrência; ou

II - na ausência de vantagem para o Contratante na manutenção do contrato, desde que o Contratante comunique ao Contratado a opção pela extinção do contrato com ao menos 2 (dois) meses de antecedência em relação à próxima data de aniversário do contrato, acarretando a extinção do contrato a partir da referida data de aniversário

contratual.

2.1.8. Ocorrendo a resolução do contrato, com base em uma das condições resolutivas estipuladas no item anterior desta cláusula, o Contratado não terá direito a qualquer espécie de indenização.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de início, conclusão, entrega, observação e recebimento do objeto, e critérios de medição, constam no Termo de Referência, que constitui parte integrante deste Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação, cessão ou transferência, total ou parcial, do objeto contratual.

CLÁUSULA QUINTA - PREÇO

5.1. O valor mensal da contratação é de R$ ..... (.....), perfazendo o valor total de R$ ..... (....).

5.1.1. O valor indicado nesta cláusula é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente demandados, medidos e fornecidos.

5.2. No valor acima estão incluídos, além do lucro, todas as despesas diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. Caso o Contratado seja optante pelo Simples Nacional e, por causa superveniente à contratação, perca as condições de enquadramento como microempresa ou empresa de pequeno porte ou, ainda, torne-se impedido de beneficiar-se desse regime tributário diferenciado por incorrer em alguma das vedações previstas na Lei Complementar nº 123, de 2006, não poderá deixar de cumprir as obrigações avençadas perante a Administração, tampouco requerer o reequilíbrio econômico-financeiro, com base na alegação de que a sua proposta levou em consideração as vantagens daquele regime tributário diferenciado.

CLÁUSULA SEXTA – PAGAMENTO (art. 92, V e VI)

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, que constitui parte integrante deste Contrato.

CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

7.1. Os preços inicialmente ajustados são fixos e irreajustáveis pelo prazo de 1 (um) ano contado da data do orçamento estimado, que corresponde a 02/04/2025.

7.2. É previsto reajuste anual dos preços inicialmente ajustados, de modo que, caso o prazo de execução do objeto contratual ultrapasse a data em que se configure 1 (um) ano a contar da data do orçamento estimado, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do IPC-FIPE -Índice de Preços ao Consumidor, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. No caso de reajuste(s) subsequente(s) ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

7.4. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante:

8.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e a documentação que o integra;

8.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, a expensas do Contratado;

8.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

8.1.5. Comunicar ao Contratado para emissão de Nota Fiscal relativa à parcela incontroversa, para efeito de liquidação e pagamento, se houver parcela incontroversa no caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, observando-se o art. 143 da Lei nº 14.133, de 2021;

8.1.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

8.1.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.8. Não praticar atos de intervenção indevida na gestão interna do Contratado, tais como (art. 48 da Lei n.º 14.133, de 2021):

I) indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

II) fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo

Contratado;

III) estabelecer vínculo de subordinação com funcionário do Contratado;

IV) definir forma de pagamento mediante exclusivo reembolso dos salários pagos;

V) demandar a funcionário do Contratado a execução de tarefas fora do escopo do objeto da contratação;

VI) Realizar outras exigências que constituam intervenção indevida da Administração na gestão interna do Contratado.

8.1.9. Cientificar a Assessoria Jurídica da Fundação CASA-SP para adoção das medidas cabíveis quando necessária medida judicial diante do descumprimento de obrigações pelo Contratado;

8.1.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, observado o prazo de 1 (um) mês para decisão, a contar da conclusão da instrução do requerimento, admitida a prorrogação motivada, por igual período, e excepcionada a hipótese de disposição legal ou cláusula contratual que estabeleça prazo específico.

8.1.11. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo Contratado no prazo máximo de 2 (dois) meses, contado a partir da conclusão da instrução do requerimento, sendo admitida a prorrogação motivada desse prazo por igual período, e observado o disposto no parágrafo único do artigo 131 da Lei nº 14.133, de 2021.

8.1.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (§4º, do art. 137, da Lei nº 14.133, de 2021).

8.1.13. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, se o caso estiver enquadrado na situação disciplinada pelo art. 93, § 3º, da Lei nº 14.133, de 2021.

8.1.14. Observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios do Contratado, a que tenha acesso durante a execução do objeto a que se refere a cláusula primeira deste contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

8.2. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro não se iniciará enquanto o Contratado não cumprir os atos ou apresentar a documentação solicitada pelo Contratante para adequada instrução do requerimento.

8.3. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus profissionais, prepostos ou subordinados.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

9.1. O Contratado deve cumprir todas as obrigações estabelecidas em lei, e aquelas constantes deste Contrato e da documentação que o integra, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a

seguir dispostas:

9.1.1. Designar e manter preposto aceito pelo Contratante para representar o Contratado na execução do contrato.

9.1.1.1. A indicação ou a manutenção do preposto do Contratado poderá ser recusada pelo Contratante, desde que devidamente justificada, hipótese em que o Contratado deverá designar outro para o exercício da atividade.

9.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II, da Lei nº 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.1.3. Alocar os profissionais necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, utilizando os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e à legislação de regência;

9.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado diretamente à Administração ou a terceiros em razão da execução do contrato, não excluindo nem reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida na documentação que integra este instrumento, o valor correspondente aos danos sofridos;

9.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante, de agente público que desempenhe(ou) função na licitação ou que atue na fiscalização ou gestão do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.1.7. Quando não for possível a verificação da regularidade no Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou em outros meios eletrônicos hábeis de informações, ou em documentação apresentada pelo Contratado para cumprimento da disciplina da fiscalização administrativa do Termo de Referência, o Contratado deverá atender a notificação para entregar ao setor responsável pela fiscalização do contrato, no prazo de 5 (cinco) dias úteis, os seguintes documentos:

1) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

2) certidões que comprovem regularidade fiscal perante as Fazendas Estadual/Distrital e/ou Municipal/Distrital do domicílio ou sede do contratado que tenham sido exigidas para fins de habilitação na documentação que integra este instrumento;

3) Certidão de Regularidade do FGTS – CRF; e

4) Certidão Negativa, ou positiva com efeitos de negativa, de Débitos Trabalhistas – CNDT.

9.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, ou Dissídio Coletivo de Trabalho das categorias abrangidas pelo contrato, e por todas as obrigações e encargos trabalhistas, previdenciários, fiscais, sociais, comerciais e os demais previstos em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante, nos termos do artigo 121 da Lei nº 14.133, de 2021;

9.1.9. Comunicar ao Fiscal do contrato, assim que possível, qualquer ocorrência anormal ou acidente que se verifique no local da execução dos serviços.

9.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto.

9.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

9.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

9.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

9.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência, observando-se o disposto no Capítulo VII do Título III da Lei nº 14.133, de 2021.

9.1.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.1.16. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz,

bem como as reservas de cargos previstas em outras normas específicas (art. 116 da Lei nº 14.133, de 2021);

9.1.18. Comprovar o cumprimento da reserva de cargos a que se refere o item anterior, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei nº 14.133, de 2021);

9.1.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização;

9.1.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros, mas que sejam previsíveis em seu ramo de atividade;

9.1.21. Cumprir as disposições legais e regulamentares federais, estaduais e municipais que interfiram na execução do objeto, bem como as normas de segurança do Contratante;

9.1.22. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida do Contratado, inclusive, a capacitação dos técnicos do Contratante ou do novo fornecedor que continuará a execução dos serviços;

9.1.23. Ceder ao Contratante todos os direitos patrimoniais relativos ao objeto contratado, o qual poderá ser livremente utilizado e/ou alterado em outras ocasiões, sem necessidade de nova autorização do Contratado.

9.2. Em atendimento à Lei nº 12.846, de 2013, e ao Decreto estadual nº 67.301, de 2022, o

Contratado se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, de modo que o Contratado não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

9.2.1. O descumprimento das obrigações previstas neste subitem poderá submeter o Contratado à extinção unilateral do contrato, a critério do Contratante, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei nº 12.846, de 2013, e o Decreto estadual nº 67.301, de 2022.

9.3. O Contratado obriga-se a não admitir a participação, na execução deste contrato, de:

9.3.1. agente público de órgão ou entidade licitante ou contratante, ou terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica, nos termos dos §§ 1º e 2º do artigo 9º da Lei nº 14.133, de 2021;

9.3.2. pessoa que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado 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, nos termos do inciso IV do artigo 14 e/ou parágrafo único do artigo 48 da Lei nº 14.133, de 2021;

9.3.3. pessoas que se enquadrem nas demais vedações previstas no artigo 14 da Lei nº

14.133, de 2021.

CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. Sempre que realizarem qualquer tipo de tratamento de dados pessoais no âmbito da execução do objeto deste contrato, as partes deverão observar as normas previstas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), com suas alterações subsequentes, e as demais normas legais e regulamentares aplicáveis.

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

11.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo

justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Garantida a prévia defesa, serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

i) Advertência, se o Contratado der causa à inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave (art. 156, § 2º, da Lei nº 14.133, de 2021);

ii) Impedimento de licitar e contratar, se praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima desta cláusula, quando não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) Declaração de inidoneidade para licitar ou contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima desta cláusula, bem como nas alíneas “b”, “c” e “d” do referido subitem, que justifiquem a imposição de penalidade mais grave (art. 156, § 5º, da Lei nº 14.133, de 2021).

iv) Multa: Calculada em conformidade com o Regulamento Anexo à Portaria Normativa nº 444/2024, que integra este instrumento.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, § 9º, da Lei nº 14.133, de 2021)

12.4. A multa poderá ser aplicada cumulativamente com as demais sanções previstas neste Contrato (art. 156, § 7º, da Lei nº 14.133, de 2021).

12.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.4.2. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, caso exigida na documentação que integra este instrumento, ou, quando for o caso, será cobrada judicialmente (art. 156, § 8º, da Lei nº 14.133, de 2021).

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, § 1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. As sanções são autônomas e a aplicação de uma não exclui a de outra.

12.8. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159 da Lei nº 14.133, de 2021).

12.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei nº 14.133, de 2021, ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160 da Lei nº 14.133, de 2021)

12.10. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no

Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161 da Lei nº 14.133, de 2021)

12.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato poderá ser extinto na forma, pelos motivos e com as consequências previstos nos artigos 137 a 139 e 155 a 163 da Lei nº 14.133, de 2021, bem como no artigo 1º, § 2º, item 3, do Decreto estadual nº 55.938, de 2010, com a redação que lhe foi dada pelo Decreto estadual nº 57.159, de 2011, na hipótese da configuração de trabalho em caráter não eventual por pessoas físicas, com relação de subordinação ou dependência, quando o contratado for sociedade cooperativa.

13.1.1. O Contratado reconhece desde já os direitos do Contratante nos casos de extinção por ato unilateral da Administração, prevista no artigo 138 da Lei nº 14.133, de 2021.

13.1.2. O contrato poderá ser extinto por algum dos motivos previstos no artigo 137 da Lei nº 14.133, de 2021, devendo a extinção ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

13.1.3. A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará a extinção contratual se não restringir sua capacidade de concluir o contrato.

13.1.3.1. Se a operação societária de que trata este subitem implicar mudança em pessoa jurídica contratada, deverá ser formalizada alteração subjetiva por termo aditivo.

13.2. O termo de extinção, sempre que possível, será precedido da indicação de:

13.2.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.2.2. Relação dos pagamentos já efetuados e ainda devidos;

13.2.3. Indenizações e multas.

13.3. A extinção do contrato não configura óbice para o reconhecimento de eventual desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

13.4. Se for constatada irregularidade no procedimento licitatório ou na execução contratual, caso não seja possível o saneamento, a decisão pelo Contratante sobre a suspensão da execução ou sobre a declaração de nulidade do contrato somente será adotada na hipótese em que se revelar medida de interesse público, observado o disposto nos artigos 147 a 149 da Lei nº 14.133, de 2021, conferindo-se ao Contratado oportunidade para prévia manifestação e participação na instrução.

CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

14.2. O Contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do Contratante, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. Se o contrato não contemplar preços unitários para serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos no artigo 125 da Lei nº 14.133, de 2021.

14.4. Eventuais alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, respeitadas as disposições da Lei nº 14.133, de 2021, admitindo-se que, nos casos de justificada necessidade de antecipação de seus efeitos, a formalização do aditivo ocorra no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

14.5. Caso haja alteração unilateral do contrato que aumente ou diminua os encargos do Contratado, o equilíbrio econômico-financeiro inicial será restabelecido no mesmo termo aditivo.

14.6. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

15.1. No presente exercício, as despesas decorrentes desta contratação correrão à conta de recursos específicos consignados no respectivo Orçamento do Estado, na dotação abaixo discriminada:

15.1.1. Gestão/Unidade: SEC. DA JUSTIÇA E CIDADANIA / FUNDAÇÃO C.A.S.A. - SEDE ADMINISTRAÇÃO - 990202;

15.1.2. Fonte de Recursos: 1.500.1.0.001;

15.1.3. Programa de Trabalho: 04.122.1729.6551.0000;

15.1.4. Elemento de Despesa: 3.3.90.40.90.

15.2. Quando a execução do contrato ultrapassar o presente exercício, a dotação relativa ao(s) exercício(s) financeiro(s) subsequente(s) será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS (art. 92, III)

16.1. Aplicam-se aos casos omissos as disposições contidas na Lei nº 14.133, de 2021, e disposições regulamentares pertinentes, e, subsidiariamente, as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, § 2º, da Lei n. 12.527, de 2011, c/c art. 22 do Decreto estadual nº 68.155, de 2023.

CLÁUSULA DÉCIMA OITAVA – FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Comarca da Capital do Estado de São Paulo para dirimir quaisquer questões que decorrerem deste Termo de Contrato, que não puderem ser resolvidas na esfera administrativa, conforme art. 92, § 1º, da Lei nº 14.133, de 2021.

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento em 01 (uma) via, que, lido e achado conforme pelo Contratado e pelo Contratante, vai por eles assinado para que

produza todos os efeitos de Direito, sendo assinado também pelas testemunhas abaixo identificadas.

Ana Claudia Carletto

Presidente

Vanessa Valente

Diretor Administrativo

Representante(s) legal do CONTRATANTE

_____

Representante legal do CONTRATADO

TESTEMUNHAS:

1- .....

2- .....

ANEXO III

PORTARIA NORMATIVA Nº 444/2024

R E G U L A M E N T O

Das Sanções Administrativas e do Processo Administrativo Sancionatório

Artigo 1º – A violação das regras estabelecidas em editais de licitação e o descumprimento de contratos de fornecimento de bens, execução de obras e prestação de serviços em que a Fundação CASA/SP figure como contratante pode ensejar a aplicação das seguintes sanções administrativas ao particular, nos termos dos artigos 156 e 162, da Lei nº 14.133/2021:

I – Advertência;

II – Multas:

a) cominatória;

b) moratória; e

c) por inexecução total ou parcial do contrato;

III – Impedimento de licitar e contratar com órgãos e entidades da Administração do Estado deSão Paulo, por até 3 (três) anos; e

IV – Declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

§ 1º – Na aplicação das sanções serão considerados:

I – A natureza e a gravidade da infração cometida;

II – As peculiaridades do caso concreto;

III – As circunstâncias agravantes ou atenuantes;

IV – Os danos que dela provierem para a Administração Pública;

V – A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

§ 2º – Os contratos poderão prever outras multas específicas, tendo em vista as peculiaridades do objeto contratado.

§ 3º – Os instrumentos convocatórios, contratos e instrumentos equivalentes deverão fazer referência expressa ao presente Regulamento, inclusive nas hipóteses de contratação direta.

Da advertência e das multas

Artigo 2º – A advertência é aplicável em caso de inexecução parcial da obrigação principal ou de obrigações acessórias, quando não se justificar a imposição de penalidade mais grave.

Artigo 3º – A multa cominatória, que tem por finalidade compelir o contratado ao cumprimento de obrigação acessória descumprida, é aplicável quando a infração contratual prejudicar a execução da obrigação principal.

Artigo 4º – A multa cominatória corresponderá a 2% (dois por cento), acrescida na seguinte proporção, conforme perdure o descumprimento:

I – Até o 30º (trigésimo) dia – 0,1% (um décimo por cento) ao dia;

II – A partir do 31º (trigésimo primeiro) dia – 0,2% (dois décimos por cento) ao dia.

Parágrafo único – A multa cominatória será calculada com base no valor contratado dos bens fornecidos ou serviços prestados / realizados no período de medição em que se verificou a infração, e não poderá exceder a 30% desse valor.

Artigo 5º – A multa moratória é aplicável quando o contratado, sem motivo justificado previamente, der causa ao descumprimento do prazo de entrega ou execução.

§ 1º – A contagem dos prazos de entrega ou execução terá início:

I – Na data fixada no instrumento contratual; ou

II – Na data de assinatura do instrumento contratual ou da retirada/envio da nota de empenho ou documento equivalente, quando não fixado outro prazo.

§ 2º – Os prazos de entrega ou execução serão contados em dias corridos, excluído o dia de inícioe incluído o do vencimento.

Artigo 6º – Cabe ao contratado solicitar, previamente ao término do prazo, a prorrogação do prazo de entrega ou execução, justificando a impossibilidade de cumprimento da obrigação no prazo inicialmente avençado.

Parágrafo único – As justificativas serão apreciadas pelo gestor do contrato, que poderá autorizara prorrogação do prazo de entrega ou execução.

Artigo 7º – Vencido o prazo de entrega ou execução, o gestor do contrato poderá:

I – Aceitar a obrigação em atraso, com aplicação da multa moratória; ou

II – Justificar o desinteresse no recebimento dos bens e/ou serviços em atraso, hipótese em que restará caracterizada a inexecução contratual.

Parágrafo único – Atrasos superiores a 60 (sessenta) dias configurarão inexecução contratual, exceto quando o gestor do contrato justificar a vantagem para a Administração na manutenção docontrato.

Artigo 8º – A multa moratória, calculada sobre o valor da obrigação cumprida em atraso, será de 2% (dois por cento), acrescida na seguinte proporção, conforme perdure a mora:

I – Até o 30º (trigésimo) dia – 0,2% (dois décimos por cento) ao dia;

II – A partir do 31º (trigésimo primeiro) dia – 0,4% (quatro décimos por cento) ao dia.

§ 1º – A multa moratória não excederá a 30% (trinta por cento) da obrigação cumprida em atraso.

§ 2º – A aplicação de multa de mora não impedirá que a Administração a converta em multa por inexecução e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas neste Regulamento.

Artigo 9º – A multa por inexecução total ou parcial do contrato, no importe de 30% (trinta por cento) do valor da obrigação não cumprida, será aplicada quando for imputável ao contratado a responsabilidade pela inexecução do contrato nas condições pactuadas e não houver interesse no recebimento da obrigação em mora.

Parágrafo único – A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Fundação CASA/SP, caracteriza o descumprimento total da obrigação assumida, sujeitando-o a multa por inexecução.

Artigo 10 – As multas serão calculadas com base no valor vigente à época da inexecução e, posteriormente, atualizadas pela variação do IPC-FIPE até a data do efetivo recolhimento.

Artigo 11 – As multas poderão ser compensadas com pagamentos eventualmente devidos pela Administração, ainda quando resultantes da execução de outro contrato, e/ou descontadas da garantia do respectivo contrato ou, quando for o caso, a Administração efetuará a cobrança judicialmente.

Das sanções restritivas do direito de licitar e contratar com a Administração

Artigo 12 – A sanção de impedimento de licitar e contratar com órgãos e entidades da Administração do Estado de São Paulo, por até 3 (três) anos, é aplicável ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII, do caput, do artigo 155, da Lei nº 14.133/2021, quando não se justificar a imposição de penalidade mais grave.

Parágrafo único – A duração da sanção será definida à luz dos critérios mencionados no § 1º, do artigo 1º, deste Regulamento, mediante justificativa baseada nos princípios da proporcionalidadee razoabilidade, observado o prazo máximo de 3 (três) anos.

Artigo 13 – A declaração de inidoneidade para licitar ou contratar com a Administração Pública direta e indireta de todos os entes federativos é aplicável ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII, do caput, do artigo 155, da Lei nº 14.133/2021, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII,do caput, do referido artigo, que justifiquem a imposição de penalidade mais grave que a sanção referida no artigo 12 acima.

Parágrafo único – A duração da sanção será definida à luz dos critérios mencionados no § 1º, do artigo 1º, deste Regulamento, mediante justificativa baseada nos princípios da proporcionalidadee razoabilidade, observado o prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

Artigo 14 – As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade poderão ser aplicadas isoladamente ou em conjunto com as penas de multa, quando cabíveis.

Do procedimento sancionatório – Disposições Gerais

Artigo 15 – A aplicação das sanções previstas neste Regulamento não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

Artigo 16 – A aplicação das sanções administrativas previstas neste Regulamento, bem como a extinção do contrato, quando cabível, serão precedidas do devido procedimento administrativo legal, destinado ao pleno exercício do contraditório e ampla defesa.

Artigo 17 – A abertura de procedimento sancionatório será impulsionada:

I – Pelo agente de contratação, em relação às infrações administrativas ocorridas durante oprocedimento licitatório; e

II – Pelo gestor do contrato, em relação às infrações administrativas ocorridas durante a execução do contrato.

§ 1º – O procedimento será inaugurado com o relato sobre a infração administrativa verificada, o seu enquadramento em uma das hipóteses legalmente previstas e, na hipótese de multa, a memória de cálculo para a sua apuração.

§ 2º – O procedimento será encaminhado, devidamente instruído, para o responsável da unidade gestora, que deliberará pela instauração do devido procedimento administrativo legal.

Artigo 18 – Instaurado o procedimento sancionatório, será promovida a intimação do particular por via postal com Aviso de Recebimento (AR), ou por qualquer meio que permita comprovar o inequívoco recebimento da intimação.

§ 1º – Considera-se inequivocamente recebida a intimação encaminhada por correspondência eletrônica, quando houver confirmação de recebimento.

§ 2º – Quando o particular sujeito à sanção não for encontrado no endereço por ele indicado no processo licitatório ou de contratação, ele será notificado por publicação no Diário Oficial do Estado.

§ 3º – O particular é responsável por manter atualizado seu endereço completo, e-mail e telefone.

§ 4º – Quando houver prestação de garantia contratual, deverá ser providenciada a notificação ao seu emitente, na forma do presente artigo, quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais, nos termos do artigo 137, §4º da Lei Federal nº 14.133/2021.

Artigo 19 – A intimação inicial deverá conter, entre outros, os seguintes elementos essenciais:

I – Descrição dos fatos que caracterizam o descumprimento das obrigações assumidas;

II – Possibilidade de caracterização de inexecução contratual e extinção do contrato, sepertinente;

III – Indicação das sanções administrativas cabíveis, com indicação dos respectivos fundamentosnormativos;

IV – Retenção de pagamentos, para compensação com eventuais multas e prejuízos causados àFundação CASA/SP, se pertinente; e

V – Previsão expressa da possibilidade de apresentação de defesa prévia nos prazos fixados nesteRegulamento.

Artigo 20 – São competentes para aplicar as sanções administrativas disciplinadas nesteRegulamento:

I – A Unidade Gestora, em relação às sanções de advertência e multas;

II – A Diretoria de Gestão Administrativa, em relação ao impedimento de licitar e contratar comórgãos e entidades da Administração do Estado de São Paulo;

III – O Presidente da Fundação CASA/SP, em relação à declaração de inidoneidade para licitar oucontratar com a Administração Pública direta e indireta de todos os entes federativos.

Artigo 21 – A aplicação das sanções administrativas previstas neste regulamento, quando apresentada defesa prévia, bem como o julgamento de recursos, serão precedidos de parecer jurídico, emitido pelo Grupo Técnico de Apoio Jurídico - GTAJ.

§ 1º – Não se aplica o disposto no caput à sanção administrativa de advertência.

§ 2º – Quando proposta a aplicação da sanção de declaração de inidoneidade para licitar e contratar com a Administração Pública, o processo será previamente encaminhado ao Grupo Técnico de Apoio Jurídico - GTAJ, independentemente da apresentação de defesa prévia ou interposição de recurso, que realizará a análise jurídica e encaminhará o procedimento ao Presidente da Fundação CASA/SP, autoridade competente para deliberar sobre a aplicação da referida sanção.

§ 3º – Em qualquer fase do procedimento sancionatório, quando houver dúvida jurídica, os autos poderão ser encaminhados ao Grupo Técnico de Apoio Jurídico - GTAJ, para análise e manifestação.

Artigo 22 – A decisão da autoridade competente será publicada na Imprensa Oficial e o interessado será intimado, nos termos do procedimento pertinente ao caso concreto.

Parágrafo único – Conforme o caso, o desfazimento do ajuste e a aplicação das penalidades cabíveis serão formalizados por meio de Termo de Rescisão Unilateral, cujo extrato será veiculado nos termos do caput.

Artigo 23 – Para fins de publicidade, as sanções aplicadas pela Fundação CASA/SP deverão serincluídas nos pertinentes cadastros de sanções administrativas, em especial:

I – Sistema Eletrônico de Registro de Sanções Administrativas em vigor; **II –** Relação de Apenados do Tribunal de Contas do Estado de São Paulo;**III –** Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS); e

IV – Cadastro Nacional de Empresas Punidas (CNEP).

Parágrafo único – Deverá o setor de contratações, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade, em especial no CEIS e no CNEP.

Do Procedimento para aplicação da pena de Advertência e/ou Multa

Artigo 24 – Verificada a situação que enseja a aplicação de advertência e/ou multa, o particular será intimado a apresentar sua defesa no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

Parágrafo único – A intimação deverá prever os elementos previstos no artigo 19 deste Regulamento, incluindo os valores referentes à multa aplicável ao caso.

Artigo 25 – Juntamente com sua defesa, o particular deverá apresentar todas as provas de suas alegações.

Artigo 26 – O procedimento será conduzido pelo gestor do contrato nos autos da respectiva contratação, cabendo à autoridade competente de que trata o artigo 20 analisar as alegações do particular e decidir motivadamente a respeito da aplicação da penalidade.

Artigo 27 – O particular será intimado da decisão, devendo constar da intimação:

I – A possibilidade de interpor recurso no prazo de 15 (quinze) dias úteis;

II – O prazo de 15 (quinze) dias úteis para o recolhimento da multa calculada, quando aplicada.

Artigo 28 – O recurso de que trata a alínea “a“ do artigo anterior será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, a qual deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

Artigo 29 – O recurso terá efeito suspensivo da decisão recorrida até que sobrevenha decisão final da autoridade competente de que trata o artigo 35.

Do procedimento para aplicação das sanções restritivas do direito de licitar e contratar com a Administração

Artigo 30 – A aplicação das sanções de impedimento para licitar e contratar com órgãos e entidades da Administração do Estado de São Paulo e de declaração de inidoneidade para licitarou contratar com a Administração Pública tramitará em procedimento específico, por meio de processo de responsabilização, instaurado por determinação do responsável da unidade gestora, que designará comissão encarregada da condução do procedimento.

Parágrafo único – A comissão a que se refere o caput será composta por 2 (dois) ou mais servidores do quadro permanente, preferencialmente com, no mínimo, 3 (três) anos de tempo de serviço na Fundação CASA/SP.

Artigo 31 – Verificada a situação que enseja a aplicação das sanções indicadas no artigo 30, a comissão deverá avaliar os fatos e circunstâncias conhecidos e intimará o particular para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

§ 1º – A comissão poderá, mediante decisão fundamentada, indeferir provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas.

§ 2º – Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o particular poderá apresentar suas alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação.

Artigo 32 – Transcorrido o prazo para apresentação da defesa prévia e finalizada a instrução, a comissão elaborará seu relatório final, no qual analisará as alegações e provas apresentadas pelo particular e opinará a respeito da caracterização da infração contratual e das penalidades cabíveis.

Artigo 33 – O relatório final será apresentado à autoridade competente, que apreciará o procedimento e, em despacho fundamentado, deliberará a respeito da aplicação das sanções inicialmente previstas.

Artigo 34 – O particular será intimado da decisão, devendo constar da intimação:

I – Da aplicação da sanção de impedimento para licitar e contratar com órgãos e entidades da Administração do Estado de São Paulo, a possibilidade de interpor recurso no prazo de 15 (quinze) dias úteis, contado da data de intimação;

II – Da aplicação da sanção de declaração de inidoneidade para licitar ou contratar com a Administração Pública, caberá apenas pedido de reconsideração, no prazo de 15 (quinze) dias úteis, contado da data de intimação;

III – O prazo de 15 (quinze) dias úteis para o recolhimento da multa calculada, quando aplicada.

§ 1º – O recurso de que trata a alínea "a" será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade competente de que trata o artigo 35, a qual deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

§ 2º – O pedido de reconsideração de que trata a alínea "b" será dirigido ao Presidente da

Fundação CASA/SP, que decidirá no prazo de 20 (vinte) dias úteis, contado do seu recebimento.

Artigo 35 – São competentes para julgar os recursos interpostos contra a aplicação das sanções administrativas previstas nesse Regulamento:

I – A Chefia de Gabinete da Presidência, em relação às sanções administrativas de advertência e demulta, quando o valor calculado for inferior ou igual a R$ 10.000,00 (dez mil reais);

II – O Presidente da Fundação CASA/SP, em relação às demais sanções administrativas.

Parágrafo único – Quando houver cumulação de sanções administrativas em relação à mesma infração administrativa, deverá ser instaurado um único procedimento sancionatório, observadas as regras de competência e de procedimento aplicáveis à sanção administrativa mais gravosa.

Artigo 36 – O recurso e o pedido de reconsideração terão efeito suspensivo da decisão recorrida até que sobrevenha decisão final da autoridade competente de que trata o artigo 35.

Artigo 37 – Os atos previstos como infrações administrativas na lei de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei federal nº 12.846/2013 serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei.

Artigo 38 – A personalidade jurídica do infrator poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos na Lei federal nº 14.133/2021 ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, a pessoa jurídica sucessora ou a empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o sancionado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia, nos termos do artigo160 do referido diploma legal.

Das Hipóteses de Retenção da Garantia e de Créditos da Contratada

Artigo 39 – Para fins de verificação quanto à liberação da garantia prestada ou pagamento dos créditos da contratada, a Administração verificará o seguinte:

I – Se houve recebimento definitivo dos bens ou serviços e se há registro de descumprimento contratual, com proposta de aplicação de multa;
II – Quando da rescisão dos contratos de serviços com regime de dedicação exclusiva de mão de obra, o fiscal administrativo deve verificar o pagamento pela contratada das verbas rescisórias ou dos documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho.

Artigo 40 – Até que a contratada comprove o disposto no artigo anterior, A Fundação CASA-SP deverá reter:

I - A garantia contratual, prestada com cobertura para os casos de descumprimento das obrigações de natureza trabalhista e previdenciária pela contratada, que será executada para reembolso dos prejuízos sofridos pela Administração, nos termos da legislação que rege a matéria;e

II - Os valores das Notas fiscais ou Faturas correspondentes em valor proporcional ao inadimplemento ou da multa proposta, até que a situação seja regularizada ou que o procedimento sancionatório seja concluído.

Artigo 41 – A Fundação CASA-SP poderá ainda:

I – Nos casos de obrigação de pagamento de multa pela contratada, reter a garantia prestada a serexecutada conforme legislação que rege a matéria; e
II– Nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, reter os eventuais créditos existentes em favor da contratada decorrentes do contrato.

Parágrafo único – Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a contratada pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente.

ANEXO IV

MODELO REFERENTE A PLANILHA DE PROPOSTA

Item	Quant.	Unid.	Descrição	Valor Mensal	Valor Total para 12 (doze) meses
1	1	Serviço	Serviços de suporte técnico e garantia onsite com renovação de licenças para soluções de segurança e infraestrutura de sustentação do DATACENTER, com manutenção corretiva e evolutiva para os equipamentos, incluindo reposição de peças e componentes		
Valor total da contratação – R$ ..... (.....).					

- Validade da proposta: **180 (cento e oitenta) dias**.

(Local e data).

_____

(Nome/assinatura do representante legal)

ANEXO V

MODELO DE DECLARAÇÃO EXIGIDA PARA HABILITAÇÃO

(em papel timbrado do licitante)

Eu, _____, portador do CPF nº _____, na condição de representante legal de _____ (nome empresarial ou denominação), interessado em participar do Pregão Eletrônico nº ___/___, Processo SEI n° ___/___, DECLARO, sob as penas da Lei, que o licitante:

a) cumpre as normas relativas à saúde e segurança no trabalho, nos termos do parágrafo único do artigo 117 da Constituição estadual; e

b) atenderá, na data da contratação, ao disposto no artigo 5º-C e se compromete a não disponibilizar empregado que incorra na vedação prevista no artigo 5º-D, ambos da Lei federal nº 6.019/1974, com redação dada pela Lei federal nº 13.467/2017, quando o caso.

(Local e data).

_____

(Nome/assinatura do representante legal)