EDITAL DE PREGÃO ELETRÔNICO N. 026/2024
PROCESSO N. 8509141-65.2024.8.06.0000

PREZADOS SENHORES,

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**, por intermédio do(a) Pregoeiro(a) e dos membros da equipe de apoio designados pela Portaria de n. 146/2022, disponibilizada no DJE, em 2/2/2022, com sede na Av. Gen. Afonso Albuquerque Lima s/n, Cambeba, CEP 60822-325, torna público para conhecimento de todos os interessados, que, no dia e hora abaixo indicados, será realizada licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, do tipo **MENOR PREÇO**, sob critério de julgamento pelo **MENOR PREÇO GLOBAL**, com modo de disputa **"ABERTO E FECHADO",** regida pela Lei Federal nº 14.133/2021, pela Lei Complementar nº 123/2006 e suas alterações, além das demais disposições legais aplicáveis e do disposto no presente Edital, com intuito de atender as necessidades deste Tribunal.

OBJETO: Contratação tem como objeto aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação, treinamento e demais especificações e características consignados, sob regime de empreitada por preço unitário, conforme especificações, quantitativos e exigências estabelecidas neste edital e seus anexos.

RECEBIMENTO DAS PROPOSTAS ATÉ: 03/07/2024 às 10:00 horas (Horário de Brasília).

ABERTURA DAS PROPOSTAS: 03/07/2024 às 10:00 horas (Horário de Brasília).

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 03/07/2024 às 10:30 horas (Horário de Brasília).

FORMALIZAÇÃO DE CONSULTAS: Observando o prazo legal, o licitante poderá formular consultas exclusivamente por e-mail, conforme endereço abaixo, informando o número da licitação.

E-mail: cpl.tjce@tjce.jus.br

REFERÊNCIA DE TEMPO: Para todas as referências de tempo será observado o horário de Brasília/DF.

Constituem Anexos deste Edital e dele fazem parte:

1 TERMO DE REFERÊNCIA
2 ORÇAMENTO DETALHADO
3 MODELO DE APRESENTAÇÃO DA PROPOSTA
4 MODELO DE DECLARAÇÃO NÃO EXTRAPOLA A RECEITA BRUTA MÁXIMA ADMITIDA PARA FINS DE ENQUADRAMENTO COMO EMPRESA DE PEQUENO PORTE.
5 MODELO DE DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE
6 MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR
7 MODELO DE DECLARAÇÃO DE ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO
8 MODELO DE DECLARAÇÃO PERCENTUAL MÍNIMO DE MÃO DE OBRA CONSTITUÍDO POR MULHERES VÍTIMAS DE VIOLÊNCIA DOMÉSTICA
9 MODELO DE DECLARAÇÃO DE QUE NÃO POSSUI, EM SUA CADEIA PRODUTIVA, EMPREGADOS EXECUTANDO TRABALHO DEGRADANTE OU FORÇADO
10 MODELO DE DECLARAÇÃO DE CUMPRIMENTO DE RESERVA DE CARGOS LEGAL PARA PESSOA COM DEFICIÊNCIA OU REABILITADO DA PREVIDÊNCIA SOCIAL
11 MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS
12 MODELO DE DECLARAÇÃO DE QUE AS PROPOSTAS ECONÔMICAS COMPREENDEM A INTEGRALIDADE DOS CUSTOS PARA ATENDIMENTO DOS DIREITOS TRABALHISTAS
13 MINUTA DO TERMO DE CONTRATO

1 DISPOSIÇÕES PRELIMINARES

1.1 O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança – criptografia e autenticação – em todas as suas fases.

1.2 Os trabalhos serão conduzidos por servidor efetivo do Tribunal de Justiça do Estado do Ceará, denominado(a) pregoeiro(a), mediante a inserção e monitoramento de dados gerados ou transferidos para o aplicativo "Licitações" constante da página eletrônica do Banco do Brasil S.A, no endereço eletrônico www.licitacoes-e.com.br.

1.3 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 do Pregoeiro em contrário, no site: www.licitacoes-e.com.br, campo "Consultar Mensagens", referente ao presente pregão eletrônico, sendo de responsabilidade do(s) licitante(s): verificar a(s) referida(s) mensagem(ns) e, ainda, os respectivos ônus por não consultá-la(s).

1.4 O Edital encontra-se à disposição dos interessados gratuitamente na Internet, nas páginas do Tribunal de Justiça do Estado do Ceará (www.tjce.jus.br), e do provedor do certame (www.licitacoes-e.com.br).

2 RECEBIMENTO E ABERTURA DAS PROPOSTAS E DATA DO PREGÃO

2.1 O licitante deverá observar as datas e os horários limites previstos para a abertura da proposta, atentando também para a data e horário para início da disputa.

3 CONDIÇÕES PARA PARTICIPAÇÃO

3.1 Poderão participar deste Pregão Eletrônico os interessados que atenderem a todas as exigências de habilitação contidas neste Edital e seus anexos, cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam, obrigatoriamente, credenciados no sistema eletrônico utilizado neste processo.

3.2 Não poderão disputar esta licitação, direta ou indiretamente, os interessados:

3.2.1 que não atendam às condições deste Edital e seu(s) anexo(s);

3.2.2 que se enquadrem nas vedações previstas no art. 14 da Lei n. 14.133/2021;

3.2.3 sob a forma de consórcio, qualquer que seja a sua constituição, exceção devidamente justificada nos autos;

3.2.4 organizados em Cooperativa, que não atenderem às prescrições artigo 16 da Lei nº 14.133/2021.

3.2.5 autores 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;

3.2.5.1 A vedação de que trata este subitem 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.

3.2.5.2 Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.2.6 que sejam 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;

3.2.6.1 a critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.2.4 e 3.2.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.2.6.2 O disposto nos itens 3.2.4 e 3.2.5 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução;

3.2.7 que sejam pessoas, física ou jurídica, que se encontrem, ao tempo da licitação, impossibilitadas de participar da licitação em decorrência de sanção que lhe foi imposta;

3.2.7.1 O impedimento de que trata este subitem 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.

3.2.8 que mantenham 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.

3.2.9 empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

3.2.10 que sejam 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;

3.2.11 que sejam agentes públicos do órgão ou entidade licitante;

3.2.11.1 Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade 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;

3.2.12 que sejam empresas estrangeiras não autorizadas a comercializar no País;

3.2.13 que sejam Organizações da Sociedade Civil de Interesse Público (OSCIP), atuando nessa condição;

3.2.14 que tenham sido declaradas inidôneas para licitar ou contratar com a Administração Pública.

3.2.15 que estejam suspensas temporariamente de participar em licitações e impedidas de contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação.

3.2.16 cujo estatuto ou contrato social não inclua dentre os objetivos sociais, atividades compatíveis com o objeto do certame.

3.2.17 que tenham em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, em atenção à Resolução do CNJ n. 7/2005 e suas alterações.

3.2.17.1 A vedação se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

3.2.17.2 A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo tribunal, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório.

3.2.17.3 É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal contratante.

3.2.18 que sejam servidores públicos ou empresas cujos dirigentes, gerentes, sócios ou componentes de seu quadro técnico sejam funcionários ou empregados públicos da Administração Pública Estadual Direta ou Indireta;

3.2.19 que sejam empresas sob a aplicação das penalidades contidas nos incisos III e IV, do art. 156, Lei n. 14.133/2021;

3.3 Não será permitida a participação de mais de uma empresa sob o controle acionário de um mesmo grupo de pessoas físicas ou jurídicas.

3.4 Considera-se participação indireta, a existência de qualquer vínculo de natureza técnica, comercial,

econômica, financeira ou trabalhista entre o autor do projeto, pessoa física ou jurídica, e o licitante ou responsável pelos serviços, fornecimentos e obras, incluindo-se os fornecimentos de bens e serviços a estes necessários.

3.5 Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei n° 14.133/2021.

3.6 A participação na licitação implica automaticamente a aceitação integral dos termos deste Edital e seus Anexos e legislação aplicável.

3.7 A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas na legislação e neste edital.

4 REGULAMENTO OPERACIONAL DO CERTAME

4.1 O certame será conduzido pelo(a) pregoeiro(a), que terá, em especial, as seguintes atribuições:

a coordenar o processo licitatório, em especial a sessão pública e o envio de lances;

b conduzir os trabalhos da equipe de apoio;

c receber, examinar e decidir as impugnações e consultas ao edital, apoiado pela área responsável pela elaboração do Termo de Referência ou do Projeto Básico;

d receber as propostas de preços;

e abrir e examinar as propostas de preços e classificar os proponentes;

f conduzir os procedimentos relativos à etapa de lances e escolher a proposta ou o lance de menor preço;

g conduzir os procedimentos relativos aos lances e à escolha da proposta do lance de menor preço;

h verificar a conformidade das propostas com os requisitos estabelecidos no instrumento convocatório;

i receber a documentação de habilitação;

j verificar e julgar as condições de habilitação;

k definir o prazo de envio de amostras de acordo com a natureza do bem licitado, quando necessário;

l declarar o vencedor;

m receber, examinar e decidir sobre a pertinência dos recursos, encaminhando-os à autoridade superior, quando mantiver sua decisão;

n adjudicar o objeto ao licitante vencedor, quando não houver recurso;

o elaborar e publicar a Ata da sessão;

p encaminhar o processo devidamente instruído à autoridade competente e propor a homologação;

q deflagrar processo administrativo para apuração de irregularidades visando à aplicação de penalidades previstas na legislação.

CREDENCIAMENTO NO APLICATIVO LICITAÇÕES

4.2 Para acesso ao sistema eletrônico, os interessados em participar do Pregão deverão dispor de chave de identificação e senha pessoal, intransferíveis, obtidas junto às Agências do Banco do Brasil S.A., sediadas no País, não sendo necessário ser cliente desta instituição bancária.

4.3 As pessoas jurídicas ou firmas individuais deverão credenciar seus representantes, mediante a apresentação de procuração por instrumento público ou particular, com firma reconhecida, atribuindo poderes para formular lances de preços e praticar todos os demais atos e operações no *licitações-e*.

4.3.1 Caso seja apresentada procuração por instrumento particular, havendo dúvida quanto à sua autenticidade, será exigido o reconhecimento de firma, nos termos do art. 12, V da Lei n. 14.133/2021.

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

4.5 A chave de identificação e a senha terão validades determinadas pelo Banco do Brasil S.A. e poderão ser utilizadas em qualquer Pregão Eletrônico realizado no *licitações-e*, sendo necessárias para formular lances de preços e praticar todos os demais atos e operações no sistema eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco do Brasil, devidamente justificada.

4.6 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 Banco do Brasil S.A, ou do Tribunal de Justiça do Ceará, por

eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.6.1 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no Sistema relacionado no item 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.

4.7 A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao Banco do Brasil S.A. para imediato bloqueio de acesso.

4.8 O credenciamento do licitante e de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes ao pregão eletrônico.

PARTICIPAÇÃO

4.9 A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha pessoal e intransferível do representante credenciado e, subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando então, encerrar-se-á automaticamente a fase de recebimento de propostas.

4.9.1 A informação dos dados para acesso deve ser feita na página inicial do site ***www.licitacoes-e.com.br*****,** opção "Acesso Identificado".

4.10 O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

4.11 O licitante que desejar utilizar-se das prerrogativas da Lei Complementar nº 123/2006, deverá declarar no campo específico do sistema que cumpre os requisitos estabelecidos no artigo 3° da referida Lei, estando apto a usufruir do tratamento favorecido constante em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133/2021.

4.11.1 A empresa que não se enquadrar nos requisitos do item ou lote exclusivo para participação de microempresas e empresas de pequeno porte, está impedida de prosseguir no certame, para aquele item ou lote;

4.11.2 A empresa que optar por não usufruir do tratamento favorecido, quando da participação em lote ou item não exclusivo para microempresas e empresas de pequeno porte, não será beneficiada com o direito ao referido tratamento, previsto na Lei Complementar nº 123/2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.11.3 A falsidade de declaração prestada objetivando os benefícios da Lei Complementar nº 123/2006, caracterizará o crime de que trata o art. 299 do Código Penal, sem prejuízo do enquadramento em outras figuras penais e das sanções previstas neste Edital.

4.12 O licitante deverá enviar sua proposta eletrônica mediante o preenchimento, obrigatório, no sistema eletrônico, do valor total de sua proposta, expresso em reais, com até 2 (duas) casas decimais e poderá mencionar, no campo "**INFORMAÇÕES ADICIONAIS**", as principais características do item ofertado, **VEDADA QUALQUER FORMA DE IDENTIFICAÇÃO DO LICITANTE, SOB PENA DE DESCLASSIFICAÇÃO**.

4.12.1 Caso não seja possível informar no campo "INFORMAÇÕES ADICIONAIS" as características do item ofertado, caberá ao licitante fornecer tais dados em arquivo anexo à proposta de preço, VEDADA QUALQUER FORMA DE IDENTIFICAÇÃO DO LICITANTE, SOB PENA DE DESCLASSIFICAÇÃO.

4.12.2 Qualquer menção a marcas de referência nos anexos deste Edital constará apenas como forma ou parâmetro de qualidade para facilitar a descrição do objeto, podendo ser substituída por marca "equivalente", "similar" ou "de melhor qualidade".

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

4.14 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos produtos.

4.15 Caberá ao licitante acompanhar as operações no sistema eletrônico, durante a sessão pública do pregão e etapas posteriores, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

4.16 Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação

anteriormente inseridos no sistema, até a abertura da sessão pública.
4.17 Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.
4.18 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.

ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES

4.19 A partir do horário previsto no sistema, terá início a sessão pública do pregão eletrônico com a divulgação das propostas de preços recebidas, passando o(a) pregoeiro(a) a avaliar a aceitabilidade das propostas. Caso ocorra alguma desclassificação, esta deverá ser fundamentada e registrada no sistema, com acompanhamento em tempo real pelos participantes.
4.20 A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.
4.21 Os preços deverão ser expressos em reais, com até 2 (duas) casas decimais em seus valores globais.
4.22 O sistema ordenará automaticamente as propostas classificadas pelo(a) pregoeiro(a) e somente estas participarão da fase de lances.
4.23 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.
4.24 Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
4.25 Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
4.26 A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência – Anexo 01 deste Edital, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.
4.27 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão encaminhados para avaliação do Pregoeiro e para acesso público após o encerramento do envio de lances.
4.28 Havendo a necessidade do envio de documentos complementares à proposta e à habilitação, necessários à confirmação daqueles exigidos neste Edital e já apresentados, serão encaminhados pelo licitante melhor classificado após o encerramento do envio de lances ou da convocação pelo pregoeiro, no prazo de 2 (duas) horas, sob pena de inabilitação.
4.29 Iniciada a etapa competitiva, na data e horário determinados neste Edital, os representantes dos fornecedores deverão estar conectados ao sistema para participar da sessão de lances e poderão encaminhar lances exclusivamente por meio do sistema eletrônico. O licitante será imediatamente informado do recebimento do lance e respectivo horário de registro e valor.
4.29.1 Para efeito de lances, será considerado o VALOR GLOBAL do lote.
4.30 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão pública e as regras estabelecidas no Edital.
4.31 O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
4.31.1 Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.
4.31.2 Durante a sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
4.32 Será adotado para o envio de lances no pregão eletrônico o modo de disputa **"ABERTO E FECHADO"**, em que os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.
4.32.1 O tempo mínimo entre lances do próprio licitante em relação ao seu último lance deverá ser de 20 (vinte) segundos, quando este não for o melhor da sala. O tempo mínimo entre licitantes em relação ao melhor lance da sala deverá ser de 3 (três) segundos.
4.33 A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até 10

(dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

4.34 Encerrado o prazo previsto no **subitem 4.33**, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um **lance final e fechado** em até 5 (cinco) minutos, que será sigiloso até o encerramento deste prazo.

4.34.1 Não havendo pelo menos três ofertas nas condições definidas neste subitem, poderão os autores dos melhores lances, na ordem de classificação, até o máximo de 3 (três), oferecer um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

4.35 Após o término dos prazos estabelecidos, o sistema ordenará os lances segundo a ordem crescente de valores.

4.35.1 Não havendo lance final e fechado classificado na forma estabelecida nos itens anteriores, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

4.36 Poderá o Pregoeiro, mediante justificativa, admitir o reinício da etapa fechada, caso nenhum licitante classificado na etapa de lance fechado atender às exigências de habilitação, para que os demais licitantes, até o máximo de três, na ordem de classificação, possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

4.37 No caso de desconexão com o(a) pregoeiro(a), no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o(a) pregoeiro(a), quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

4.38 Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão será suspensa, sendo reiniciada somente decorridas 24 (vinte e quatro) horas após comunicação do fato pelo(a) pregoeiro(a) aos participantes, por meio de mensagem no sistema, divulgando data e hora da reabertura da sessão.

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

4.40 Após o encerramento dos lances, o sistema detectará a existência de situação de empate ficto. Em cumprimento ao que determina a Lei Complementar nº 123/2006, a microempresa, a empresa de pequeno porte e a cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, e que ofertou lance de até 5% (cinco por cento) superior ao menor preço da arrematante que não se enquadre nessa situação de empate, será convocada automaticamente pelo sistema, na sala de disputa, para, no prazo de 5 (cinco) minutos, utilizando-se do direito de preferência, ofertar novo lance inferior ao melhor lance registrado, sob pena de preclusão.

4.41 Não havendo manifestação da licitante, o sistema verificará a existência de outro em situação de empate, realizando o chamado de forma automática. Não havendo outra situação de empate, o sistema emitirá mensagem, cabendo ao pregoeiro dar por encerrada a disputa do lote.

4.42 O sistema informará a proposta de menor preço ao encerrar a fase de disputa, quando for o caso, após negociação e decisão pelo(a) pregoeiro(a) acerca da aceitação do lance de menor valor.

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

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

4.45 Somente haverá empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

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

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

4.46.2 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 nesta Lei;

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

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

4.47 Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou

prestados por:

4.47.1 empresas estabelecidas no território do Estado do Ceará;

4.47.2 empresas brasileiras;

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

4.47.4 empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187/2009.

DA LICITANTE ARREMATANTE

4.48 Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o(a) pregoeiro(a) poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

4.48.1 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.

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

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

4.48.4 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.

4.49 É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

4.50 Após a negociação do preço, o(a) Pregoeiro(a) iniciará a fase de aceitação e julgamento da proposta.

4.51 Encerrada a etapa de negociação da proposta, o Pregoeiro examinará a proposta classificada provisoriamente em primeiro lugar quanto à compatibilidade da proposta de preço em relação ao valor estimado e à adequação do objeto **(fase de aceitação e julgamento da proposta)**. Em seguida, verificará também o cumprimento às demais exigências para habilitação contidas neste Edital.

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

4.52 Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e o valor estimado para a contratação, inclusive, quanto aos preços unitários.

4.53 Constatando o atendimento das exigências fixadas no Edital, o objeto será adjudicado ao autor da proposta ou lance de menor preço.

5 DA ACEITABILIDADE DA PROPOSTA

5.1 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 14.133/2021, legislação correlata e no item 7 deste edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação.

5.1.1 Junto a sua proposta a licitante deverá encaminhar a declaração de responsabilidade pela autenticidade dos documentos apresentados, conforme **Anexo 11 – Declaração de autenticidade da documentação deste edital**.

5.1.2 Constatada a ausência da declaração de autenticidade da documentação, não implicará no afastamento imediato da arrematante por considerar-se falha formal passível de saneamento nos termos deste edital.

5.1.3 O não cumprimento da entrega da documentação, nos prazos estabelecidos neste Edital, acarretará desclassificação/inabilitação, bem como poderá acarretar a aplicação das sanções estabelecidas na Lei Nacional nº 14.133/2021, sendo convocado o licitante subsequente, e, assim, sucessivamente, observada a ordem de classificação.

5.1.4 Caso o arrematante venha a ser desclassificado ou inabilitado, o(a) pregoeiro(a) convocará os demais participantes, seguindo a ordem de classificação, devendo suas propostas de preços serem entregues no prazo máximo de 2 (duas) horas, contados da sua convocação realizada por meio do sistema de licitações.

5.2 Será verificado eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante consulta aos seguintes cadastros:

5.2.1 Certificado de Registro Cadastral (CRC-Ce).

5.2.2 Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

5.2.3 Cadastro Nacional de Empresas Punidas (CNEP), mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

5.3 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429/1992.

5.4 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.

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

5.4.2 O licitante será convocado para manifestação previamente a uma eventual desclassificação.

5.4.3 Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

5.5 Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

5.6 Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o **subitem 4.11** deste edital.

5.7 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.

5.7.1 A não apresentação de declarações formais e/ou termos de compromissos exigidos, inclusive aqueles relativos à habilitação, não implicarão desclassificação ou inabilitação imediata da licitante. Compete o pregoeiro conceder prazo razoável para o devido saneamento, em respeito aos princípios do formalismo moderado e da razoabilidade.

5.7.2 A ausência de documentos, caso haja possibilidade de consulta em sites oficiais, não será considerada motivo de desclassificação.

5.8 Será desclassificada a proposta vencedora que:

5.8.1 contiver vícios insanáveis;

5.8.2 não obedecer às especificações técnicas contidas no Termo de Referência

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

5.8.4 não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

5.8.5 apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

5.9.1 A inexequibilidade, na hipótese de que trata o **subitem 5.9**, só será considerada após diligência do pregoeiro que comprove:

5.9.1.1 que o custo do licitante ultrapassa o valor da proposta; e

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

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

5.11 Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

5.11.1 Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva cuja produtividade seja mensurável e indicada pela Administração, o licitante deverá indicar a

produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

5.11.2 Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade.

5.11.3 Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

5.12 Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo licitante, no prazo indicado pelo sistema, desde que não haja majoração do preço.

5.12.1 O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas, respeitado o valor máximo admitido pela administração para os itens;

5.13 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.

5.14 A proposta deverá explicitar:

5.14.1 Nome, endereço, CNPJ e inscrição estadual/municipal;

5.14.2 Número do processo e do Pregão;

5.14.3 Planilha de preço por itens, em conformidade com o **Anexo 2** deste Edital;

5.14.4 Descrição do objeto da presente licitação, em conformidade com as exigências contidas neste edital e seus anexos;

5.14.5 O prazo de validade que não será inferior a 90 (noventa) dias, contados a partir da data da sua apresentação, razão pela qual a não manutenção das propostas no decorrer de seu prazo de validade poderá ensejar as sanções previstas no art. 90, §5º da Lei n. 14.133/2021;

5.14.6 Valor(es) unitário(s) e total(is) com até 2 (duas) casas decimais, conforme **Anexo 2** deste Edital, devendo os valores totais serem escritos em numeral e por extenso.

5.15 No caso de a proposta de preços da proponente vencedora necessitar de ajuste para sanar evidente erro material, incluindo-se o caso de apresentar erros de multiplicação, somas e outros, o pregoeiro poderá fixar prazo máximo de 2 (dois) dias úteis para reenvio da proposta ajustada a contar da solicitação feita por meio do sistema eletrônico do Banco do Brasil.

5.16 Ocorrendo discordância entre os valores numéricos e, por extenso, prevalecerão estes últimos.

6 JULGAMENTO DAS PROPOSTAS

6.1 Para julgamento, será adotado o critério de **MENOR PREÇO GLOBAL**, observados os prazos para execução, as especificações técnicas, parâmetros mínimos de desempenho e de qualidade e demais condições definidas neste edital.

6.2 A proposta final não poderá conter item com valor unitário superior ao estimado pela Administração, descrito no **Anexo 2 do Edital**, sob pena de desclassificação, independentemente do valor total da proposta.

6.3 Após a apresentação da Proposta, não caberá desistência.

6.4 Serão desclassificadas as propostas que conflitem com as normas deste edital ou da Legislação em vigor.

6.5 Serão rejeitadas as propostas que:

6.5.1 sejam incompletas, isto é, não contenha(m) informação(ões) suficiente(s) que permita(m) a perfeita identificação do objeto licitado;

6.5.2 contiverem preços superiores aos praticados no mercado ou comprovadamente inexequíveis.

6.5.3 contiverem qualquer limitação ou condição substancialmente contrastante com o presente edital e seus anexos, ou apresentarem Proposta de Preços com preços manifestamente inexequíveis;

6.6 Será desclassificada a proposta que não corrigir ou não justificar eventuais falhas apontadas pelo(a) Pregoeiro(a).

6.7 A desclassificação será sempre fundamentada e registrada no sistema.

6.8 De conformidade com parecer da COPECON, não constituirá causa de desclassificação do(a) proponente a irregularidade formal que não afete o conteúdo ou a idoneidade da proposta e/ou documentação.

6.9 No julgamento das propostas, o(a) Pregoeiro(a) poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

6.10 Se a proposta de menor preço não for aceitável, ou se a licitante deixar de reenviá-la, ou, ainda, se o

licitante desatender às exigências habilitatórias, o(a) pregoeiro(a) examinará a proposta subsequente, verificando sua compatibilidade e a habilitação do participante, na ordem de classificação, e, assim, sucessivamente, até a apuração de uma proposta que atenda aos requisitos deste edital.

6.11 O licitante remanescente que esteja enquadrado no percentual estabelecido no art. 44, §2º, da Lei Complementar n. 123/2006, no dia e hora designados, será convocado na ordem de classificação, para ofertar novo lance inferior ao melhor lance registrado no lote, e, no prazo de 5 (cinco) minutos, utilizar-se do direito de preferência.

6.12 Havendo aceitação da proposta classificada em primeiro lugar quanto à compatibilidade de preço, o pregoeiro avaliará as condições de habilitação da licitante.

7 HABILITAÇÃO

7.1 Os licitantes deverão apresentar os seguintes documentos de habilitação para participar do presente certame:

7.1.1 No caso de licitante CADASTRADO, o Certificado de Registro Cadastral (CRC) emitido pela Secretaria do Planejamento e Gestão (SEPLAG), do Estado do Ceará, compatível com o ramo do objeto licitado;

7.1.1.1 A Comissão Permanente de Contratação do TJCE verificará eletronicamente a situação do licitante no Certificado de Registro Cadastral (CRC). Caso esteja com algum documento vencido, deverá apresentá-lo juntamente com os documentos de habilitação, sob pena de inabilitação, salvo os documentos acessíveis para consultas em sítios oficiais que poderão ser consultados pelo(a) pregoeiro(a).

7.1.1.2 Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao CRC.

7.1.1.3 Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema, o licitante será inabilitado, ressalvado o disposto quanto à comprovação da regularidade fiscal das microempresas, empresas de pequeno porte, conforme estatui o art. 43, §1º da Lei Complementar n. 123/2006.

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

7.1.1.4 Caso a **microempresa ou empresa de pequeno porte** tenha registro no CRC a sua certidão simplificada, expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte.

I Na hipótese de no documento não constar expressamente o prazo de validade determinado, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de 30 (trinta) dias, contados a partir da data de sua emissão.

7.1.2 O licitante NÃO CADASTRADO no CRC junto à SEPLAG/CE deverá apresentar os documentos relacionados na opção "Informações sobre Cadastramento de Fornecedores" disponíveis no *sítio:* www.portalcompras.ce.gov.br, relativos à Habilitação Jurídica e à Regularidade Fiscal e trabalhista, nas condições seguintes:

7.1.2.1 Habilitação jurídica:

a No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

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

c Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

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

e No caso de **microempresa ou empresa de pequeno porte**: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte.

I Na hipótese de no documento não constar expressamente o prazo de validade determinado, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou

regulamentação, o documento será considerado válido pelo prazo de 30 (trinta) dias, contados a partir da data de sua emissão.

f No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização.

7.1.2.2 Regularidade fiscal e trabalhista:

a Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

b 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 n. 1.751, de 2.10.2014, e suas alterações, da Secretaria da Receita Federal do Brasil e da Procuradoria-Geral da Fazenda Nacional;

c Prova de regularidade com a Seguridade Social (INSS);

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

e 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 n. 5.452/1943;

f Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto desta licitação;

g Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante.

h Prova de regularidade de Tributos Municipais.

7.1.3 Caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei;

7.1.4 Caso o licitante detentor do menor preço seja microempresa, empresa de pequeno porte enquadrada no artigo 34 da Lei n. 11.488/2007, deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

7.1.5 Declaração do licitante, se couber, quanto às microempresas e às empresas de pequeno porte, que, no ano-calendário de realização da licitação, **ainda não celebraram contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida** para fins de enquadramento como empresa de pequeno porte, **conforme modelo no Anexo 4 do Edital**;

7.1.6 Declaração do licitante, se couber, tratar-se de **microempresa ou empresa de pequeno porte**, **conforme modelo no Anexo 5 do Edital**;

7.1.6.1 O licitante organizado em **cooperativa deverá declarar**, ainda, **que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133/2021**.

7.1.7 Ato constitutivo, estatuto ou contrato social em vigor, caso o representante legal da empresa integre seu quadro societário;

7.1.8 Procuração, acompanhada do ato constitutivo, estatuto ou contrato social em vigor, no caso do representante legal da empresa ser procurador;

7.1.9 Declaração que não possui em seu quadro funcional menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, menores de 16 (dezesseis) anos em trabalho algum, salvo na condição de aprendiz a partir de 14 (quatorze) anos, **conforme Anexo 6 do Edital**;

7.1.10 Declaração de atendimento aos requisitos de habilitação, **conforme Anexo 7 do Edital**;

7.1.11 Declaração de que atenderá às disposições sobre o quantitativo mínimo de mão de obra constituído por mulheres vítimas de violência doméstica, em percentual mínimo de 8 (oito) por cento das vagas, **conforme modelo constante no Anexo 8 do Edital** (Declaração exigível, exclusivamente, em licitações de serviços contínuos com regime de dedicação exclusiva de mão de obra).

7.1.12 Declaração de que não possui, em sua cadeia produtiva, empregados executando **trabalho degradante ou forçado**, conforme modelo **constante no Anexo 9 do Edital**.

7.1.13 Declaração de cumprimento de **reserva de cargos legal** para pessoa com deficiência ou reabilitado da previdência social, conforme modelo **constante no Anexo 10 do Edital**.

7.1.13.1 Quando a licitante não estiver obrigada ao atendimento da reserva de cargos mencionada, nos termos do art. 93 da Lei Federal n. 8.213, de 24 de julho de 1991, deverá apresentar declaração relativa à isenção da citada obrigatoriedade.

7.1.14 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, conforme modelo **constante no Anexo 12 do Edital.**

7.2 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência conforme art. 64 da Lei nº 14.133/2021.

7.2.1 Não se caracterizam documentos novos aqueles que venham a comprovar fatos existentes à época da abertura da sessão, com respaldo no previsto no Acórdão 1211/2021-TCU-Plenário.

7.2.2 O(s) documento(s) referente(s) ao subitem anterior deverá(ão) constar em um único arquivo apresentado após a solicitação do pregoeiro.

7.2.3 A não apresentação dos referidos documentos nos prazos fixados ensejará a desclassificação da proposta.

QUALIFICAÇÃO TÉCNICA E ECONÔMICO-FINANCEIRA

7.3 O licitante deverá satisfazer às condições de **qualificação técnica** descritas no **subitem 12.4 conforme ANEXO I deste Edital de Pregão Eletrônico.**

7.3.1 A comprovação da Capacitação Técnico-operacional da empresa licitante deverá ser fornecida pela pessoa jurídica contratante dos serviços a que se refere o atestado, não sendo admitido atestado fornecido por terceiros.

7.3.2 O atestado deverá estar assinado por profissional habilitado, devidamente identificado, com poderes de representação, sendo acompanhado da documentação comprobatória correspondente.

7.4 Para efeitos de comprovação da **qualificação econômico-financeira**, o licitante deverá atender ao **subitem 12.3 conforme ANEXO I deste Edital** e apresentar:

a Certidão Negativa expedida pelo Cartório Distribuidor de Falência e Recuperação Judicial do local da sede da licitante, com data de expedição não superior a 60 (sessenta) dias, quando não houver prazo de validade expresso no documento.

b Patrimônio líquido contabilizado de, no mínimo, 10% (dez por cento) do valor total estimado da contratação, comprovado por meio da apresentação do Balanço patrimonial dos 2 (dois) últimos exercícios sociais, já exigível e apresentado na forma da lei, que comprove a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 3 (três) meses da data da apresentação da proposta.

1 O balanço patrimonial deverá estar assinado pelo responsável legal da empresa e pelo responsável por sua elaboração, Contador ou outro profissional equivalente devidamente registrado no Conselho Regional de Contabilidade.

2 Se necessária a atualização do balanço e do patrimônio líquido, deverá ser apresentado o memorial de cálculo correspondente, juntamente com os documentos em apreço.

3 O balanço patrimonial deverá estar registrado ou na Junta Comercial ou no Registro Civil das Pessoas Jurídicas ou no Sistema Público de Escrituração Digital – SPED, para as empresas que utilizem o sistema eletrônico de escrituração e que tenham seus documentos registrados na Junta Comercial.

4 A apresentação do balanço patrimonial, da demonstração de resultado de exercício e das demais demonstrações contábeis serão dos 2 (dois) últimos exercícios sociais.

5 Os documentos referidos no **subitem 7.4 "b"** limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há **menos de 2 (dois) anos.**

c A boa situação econômico-financeira da empresa será avaliada pelos seguintes indicadores, obtidos do balanço patrimonial apresentado:

1 Os índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) devem ser maiores que 1,00 (um), e resultantes da aplicação das seguintes fórmulas:

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

$$SG = \frac{\text{ATIVO TOTAL}}{}$$

$$LC = \frac{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}{\text{ATIVO CIRCULANTE}}$$
$$\text{PASSIVO CIRCULANTE}$$

2 As fórmulas dos índices contábeis referidos deverão estar devidamente aplicadas em memorial de cálculos juntado ao balanço, calculado com 2 (duas) casas decimais, sem arredondamento.

3 A fonte de informação dos valores considerados deverá ser o Balanço Patrimonial, apresentado na forma da lei.

7.4.1 A Comissão de Contratação não efetuará o cálculo dos índices exigidos no **subitem 7.4 "c"** deste Edital, o qual deverá ser efetuado e assinado por profissional de contabilidade devidamente registrado, não sendo admitida a não apresentação dos índices e do cálculo sob a alegativa de que os dados constam no balanço apresentado.

7.4.2 Para efeito dos cálculos prescritos nestes requisitos de qualificação econômico-financeira será considerado o ano fiscal, na forma da lei;

7.4.3 O Tribunal de Justiça reserva-se o direito de realizar diligências, para aferir a exequibilidade das propostas ou exigir dos licitantes que ela seja demonstrada do licitante, nos termos do art. 59, §2º, da Lei Nacional n. 14.133/2021.

7.4.4 A análise de documentos para efeitos de qualificação técnica e econômico-financeira pautar-se-á pela observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.

7.5 Os documentos de habilitação deverão ser apresentados da seguinte forma:

7.5.1 Obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos tanto para matriz como para todas as filiais. A contratação será celebrada com a sede que apresentou a documentação;

7.5.2 Caso apresentados em qualquer processo de fotocópia, deverão vir em cópias autenticadas em cartório ou em cópias simples acompanhadas de originais, conforme Provimento do TJCE nº 15/2008 c/c Lei Nacional n. 13.726, de 8 de outubro de 2018, sob pena de não o fazendo, serem consideradas inabilitadas no presente processo licitatório;

7.5.2.1 A prova de autenticidade de cópia de documento público ou particular poderá ser feita perante agente de contratação do TJCE, mediante apresentação de original ou de declaração de autenticidade por advogado, sob sua responsabilidade pessoal.

7.5.3 Os documentos obtidos através de sítios oficiais que estejam condicionados à aceitação via internet terão sua autenticidade verificada pelo(a) pregoeiro(a). Os documentos de habilitação disponibilizados pelos Órgãos competentes emitidos por meio eletrônico através da rede mundial de computadores (internet), para fins de julgamento, serão considerados originais, não necessitando de autenticação notarial. Outrossim, se estes forem apresentados através de cópias xerográficas, estas deverão obrigatoriamente ser autenticadas em cartório ou acompanhados de originais;

7.5.4 Caso haja documentos redigidos em idioma estrangeiro, estes serão somente considerados se acompanhados da versão em português, firmada por tradutor.

7.5.5 Dentro do prazo de validade. Na hipótese de no documento não constar expressamente o prazo de validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. Na ausência de tal declaração ou regulamentação, o documento será **considerado válido pelo prazo de 30 (trinta) dias**, contados a partir da data de sua emissão.

7.6 O(A) Pregoeiro(a) poderá também solicitar originais de documentos já autenticados para fins de verificação, sendo a empresa obrigada a apresentá-los no prazo **de 2 (dois) dias úteis**, contados a partir da solicitação, sob pena de não o fazendo, ser inabilitada.

7.7 Todas as certidões negativas apresentadas deverão comprovar a quitação com os tributos pertinentes, as que se encontram positivas só serão acatadas se tiverem o mesmo valor das negativas.

7.8 Em se tratando de microempresa ou empresa de pequeno porte, esta deverá apresentar todos os documentos exigidos para efeito de comprovação da regularidade fiscal, mesmo que estes apresentem

alguma restrição, conforme determina o art. 43, da Lei Complementar n. 123/2006;

7.8.1 Havendo alguma restrição na comprovação da regularidade fiscal da microempresa ou empresa de pequeno porte, será assegurado o prazo de **5 (cinco) dias úteis**, contados da data em que o proponente for declarado vencedor do certame, prorrogável por igual período, a critério da Administração, para a regularização da situação que deu causa à restrição;

7.8.2 A não regularização no prazo previsto no subitem anterior implicará a decadência do direito à contratação sem prejuízo das sanções previstas neste edital.

7.9 Constatando o atendimento das exigências previstas no Edital, o licitante será declarado vencedor, sendo-lhe adjudicado o objeto da licitação pelo(a) próprio(a) pregoeiro(a), na hipótese de inexistência de recursos administrativos ou pela Autoridade Superior, na hipótese de existência de recursos administrativos.

7.10 Se o licitante desatender às exigências previstas neste **item 7 (sete)**, o(a) pregoeiro(a) examinará a oferta subsequente na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação, repetindo esse procedimento sucessivamente, se for necessário, até a apuração de uma proposta que atenda ao edital, sendo o respectivo licitante declarado vencedor.

7.11 Da sessão, o sistema do Banco do Brasil S/A gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes, bem como serão registrados nos autos do processo administrativo descrito no preâmbulo deste Edital.

8 PEDIDOS DE ESCLARECIMENTOS E IMPUGNAÇÕES AO EDITAL

8.1 Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao(à) pregoeiro(a), até **3 (três) dias úteis** anteriores à data fixada para abertura das propostas, exclusivamente por meio eletrônico, no endereço cpl.tjce@tjce.jus.br, informando o número deste pregão no sistema do Banco do Brasil e o órgão interessado.

8.2 Até **3 (três) dias úteis** anteriores à data fixada para abertura das propostas, qualquer pessoa poderá impugnar o presente edital, mediante petição por escrito, protocolizada no Tribunal de Justiça do Estado do Ceará, por meio do correio eletrônico: cpl.tjce@tjce.jus.br;

8.2.1 Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente.

8.3 A resposta à impugnação ou ao pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

8.4 A impugnação não terá efeito suspensivo que poderá ser concedido por decisão motivada do(a) pregoeiro(a).

8.5 Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

9 DOS RECURSOS ADMINISTRATIVOS

9.1 Do ato que encerra o julgamento das propostas ou do ato de habilitação ou inabilitação de licitante, o proponente que desejar recorrer contra decisões do(a) Pregoeiro(a), poderá fazê-lo de imediato e motivadamente, até **2 (duas) horas** do mencionado ato, manifestando sua intenção com o registro da síntese das suas razões, exclusivamente no âmbito do sistema eletrônico, sendo-lhe concedido **prazo de 3 (três) dias** para apresentar por escrito as razões do recurso, conforme o art. 165 da Lei nº 14.133, de 2021, devidamente protocolizadas no Tribunal de Justiça do Estado do Ceará, no endereço eletrônico constante no preâmbulo deste edital. Os demais licitantes ficam, desde logo, convidados a apresentar contrarrazões em igual número de dias, que começarão a correr da data da intimação pessoal ou da divulgação da interposição do recurso.

9.1.1 O prazo para apresentação das razões recursais será iniciado na data de intimação ou da lavratura da habilitação ou inabilitação;

9.1.2 A falta de manifestação imediata e motivada importará a preclusão do direito de recurso.

9.2 Fica assegurada aos licitantes vista imediata dos autos do Pregão, com a finalidade de subsidiar a preparação de recursos e de contrarrazões. Os referidos Autos estarão disponíveis na sala da Comissão de Contratação do TJCE.

9.3 Não serão conhecidos os recursos intempestivos, nem acolhidas razões ou contrarrazões não enviadas nos termos prescritos neste edital.

9.4 Os recursos poderão ser encaminhados em campo próprio do sistema.

9.5 Os recursos subscritos por representantes deverão ser acompanhados por documento comprobatório da habilitação legal.

9.6 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida.

9.7 Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente.
9.8 O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.
9.9 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
9.10 A decisão em grau de recurso será definitiva e dela dar-se-á conhecimento aos interessados, por meio de comunicação via e-mail.

10 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

10.1 A adjudicação dar-se-á pelo pregoeiro quando não ocorrer interposição de recursos que encaminhará o processo devidamente instruído à autoridade competente e propor a homologação. Caso contrário, a adjudicação ficará a cargo da autoridade competente.
10.2 Não havendo interposição de recursos por parte dos licitantes o pregoeiro poderá adjudicar o objeto ao licitante vencedor, encaminhando em seguida o processo para homologação pela autoridade competente.
10.3 Havendo recurso(s), depois de decididos e constatada a regularidade dos atos praticados, a autoridade competente poderá adjudicar o objeto ao licitante vencedor e homologar a licitação.
10.4 A homologação da licitação é de responsabilidade da autoridade competente e só poderá ser realizada depois da adjudicação do objeto ao vencedor.
10.4.1 A homologação do resultado desta licitação não implicará direito à contratação.
10.5 O sistema gerará Ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.
10.6 Após a homologação, o licitante vencedor será convocado para assinar o contrato ou a ata de registro de preços no prazo definido neste edital.
10.7 Na assinatura do termo de contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas neste edital, as quais deverão ser mantidas pelo licitante durante a vigência do termo de contrato ou da ata de registro de preços.

11 SANÇÕES ADMINISTRATIVAS

11.1 Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:
11.1.1 deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo pregoeiro ou pelo órgão ou entidade demandante da licitação, em sede de diligência;
11.1.2 salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:
11.1.2.1 não enviar a proposta adequada ao último lance ofertado ou após a negociação;
11.1.2.2 recusar-se a enviar o detalhamento da proposta quando exigível;
11.1.2.3 pedir para ser desclassificado quando encerrada a etapa competitiva;
11.1.2.4 deixar de apresentar amostra;
11.1.2.5 apresentar proposta (ou amostra) em desacordo com as especificações do edital;
11.1.3 não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
11.1.4 recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;
11.1.5 apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;
11.1.6 fraudar a licitação;
11.1.7 comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
11.1.7.1 agir em conluio ou em desconformidade com a lei;
11.1.7.2 induzir deliberadamente a erro no julgamento;
11.1.7.3 apresentar amostra falsificada ou deteriorada;
11.1.7.4 praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
11.1.7.5 praticar ato lesivo previsto no art.5º da Lei nº. 12.846/2013.
11.2 A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no **subitem 11.1.4**, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.
11.2.1 A exigência da garantia de que trata o subitem anterior, obedecerá ao disposto no art. 58 da Lei nº

14.133/2021.

11.3 Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar a contratada as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

11.3.1 advertência;

11.3.2 multa;

11.3.3 impedimento de licitar e contratar; e

11.3.4 declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade;

11.4 Na aplicação das sanções serão considerados(as):

11.4.1 a natureza e a gravidade da infração cometida;

11.4.2 as peculiaridades do caso concreto;

11.4.3 as circunstâncias agravantes ou atenuantes;

11.4.4 os danos que dela provierem para a Administração Pública;

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

11.5 A sanção de multa calculada na forma do edital ou do contrato, não será inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.

11.5.1 A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o complementem, às sanções e penalidades administrativas, inclusive multas, conforme previsão da **Cláusula Dez do Anexo 13 – Termo de Contrato**, sem prejuízo das sanções legais e responsabilidades civil e criminal.

11.5.2 A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

11.5.3 Os percentuais de multas aplicadas incidirão sobre o valor global do termo de contrato licitado ou celebrado, quando moratórias.

11.6 As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

11.7 Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.8 A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos **subitens 11.1.1, 11.1.2 e 11.1.3**, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

11.9 Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos **subitens 11.1.4, 11.1.5, 11.1.6, 11.1.7 e 11.1.8**, bem como pelas infrações administrativas previstas nos **subitens 11.1.1, 11.1.2 e 11.1.3** que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

11.10 A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.11 Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual 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, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

11.12 Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

11.13 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14 A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de

reparação integral dos danos causados.

11.15 Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

11.16 As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.

11.17 Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

11.18 Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a Administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 156 da Lei n. 14.133/21:

11.18.1 Aplicação de multa administrativa, além das Glosas previstas neste documento.

11.18.1.1 Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo.

11.18.1.2 Na ordem de 0,5% do valor total da contratação, ao dia de suspensão ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços contratados ao total de 10%, moratório.

11.18.1.3 Caso os limites do subitem anterior sejam excedidos, configura-se então casos de inexecução contratual.

12 DA GARANTIA CONTRATUAL

12.1 Será exigida a prestação de garantia na presente contratação, conforme regras constantes na **Cláusula Nona do Anexo 13 – Minuta do Termo de Contrato deste Edital**.

12.2 A CONTRATADA deverá entregar ao Gerente de Contratação do objeto, que submeterá à Coordenadoria Central de Contratos e Convênios do TJCE, **no prazo prescrito no art. 96 da Lei n.º 14.133/2021**, a título de garantia, a quantia equivalente a 5% (cinco por cento) do valor global da contratação, cabendo-lhe optar dentre as modalidades previstas no **art. 96, Lei n.º 14.133/2021**.

12.3 A garantia será devolvida à CONTRATADA somente depois do cumprimento integral das obrigações assumidas, inclusive recolhimento de multas e satisfação de prejuízos causados ao CONTRATANTE.

12.4 Será concedido prazo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para a prestação da garantia pelo contratado quando optar pela modalidade seguro-garantia.

12.5 A garantia deverá ter validade, expressa na apólice, durante a execução do contrato acrescida de 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação.

12.6 A ausência de prestação da garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa e rescisão unilateral do contrato administrativo.

13 DA GARANTIA DO SERVIÇO (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

13.1 A garantia contratual dos serviços, complementar à garantia legal, deve atender as especificações técnicas **dos itens 5.11.6.1, 4, 13 e 15 conforme ANEXO I deste Edital,** pelo prazo mínimo contratual de 60 (sessenta) meses, contado a partir do primeiro dia útil subsequente à data do Termo de Recebimento Definitivo (TRD).

14 DA CONTRATAÇÃO

14.1 As obrigações decorrentes da presente licitação serão formalizadas por instrumento de contrato, conforme **minuta constante do Anexo 13 deste Edital**, celebrado entre o Tribunal de Justiça do Estado do Ceará, denominado CONTRATANTE, e a adjudicatária, denominada CONTRATADA, que observará os termos da Lei n. 14.133/2021, deste Edital e demais normas pertinentes.

14.2 O adjudicatário terá o **prazo de 5 (cinco) dias úteis**, contados a partir da data de sua convocação expedida pelo CONTRATANTE, para assinar o Termo de Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

14.3 Prazo de vigência contratual será de 60 (sessenta) meses, contados da assinatura do termo de contrato, podendo ser prorrogado até limite permitido pela Lei 14.133/21 e conforme a conveniência estabelecida entre CONTRATADA e CONTRATANTE.

14.4 Na assinatura do termo de contrato será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do termo de contrato.
14.5 O presente Edital e seus anexos, bem como a proposta de preços serão partes integrantes da contratação.

15 DO PAGAMENTO

15.1 As condições de pagamento estão descritas no **subitem 8.6 do ANEXO I deste Edital de Pregão Eletrônico.**
15.2 Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0{,}00016438$$

no qual i = taxa percentual anual no valor de 6% (seis por cento).

16 DO REAJUSTAMENTO E DOS RECURSOS FINANCEIROS

16.1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.
16.2 Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do **Índice de Custo da Tecnologia da Informação (ICTI) - Ipea**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
16.3 O processo referente ao pedido de reajuste supra, deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.
16.4 Os recursos financeiros serão decorrentes do financiamento contraído junto ao Banco Interamericano de Desenvolvimento – BID, no âmbito do Programa de Modernização do Poder Judiciário do Estado do Ceará (PROMOJUD), tendo como fonte os Recursos de Operações de Crédito, nas seguintes dotações orçamentárias:

04200021.02.126.192.11470.15.449052.1.759.1200070.1.20 (00475)
04200021.02.126.192.11470.15.449052.2.759.1200070.1.20 (-)
04200021.02.126.192.20511.15.339040.1.759.1200070.1.20 (08290)
04200021.02.126.192.20511.15.339040.2.759.1200070.1.20 (-)
04200021.02.126.192.20512.15.339040.1.759.1200070.1.20 (23584)
04200021.02.126.192.20512.15.339040.2.759.1200070.1.20 (-)

16.5 Nenhuma contratação será efetuada sem a prévia indicação da disponibilidade orçamentária.

17 DAS OBRIGAÇÕES DO TJCE

17.1 As obrigações do TJCE estão estabelecidas no **item 6 do ANEXO I deste Edital.**

18 DAS OBRIGAÇÕES DA CONTRATADA

18.1 As obrigações da CONTRATADA estão estabelecidas no **item 7 do ANEXO I deste Edital.**

19 DISPOSIÇÕES FINAIS

19.1 A presente licitação não importa necessariamente em contratação, podendo o Tribunal de Justiça do Estado do Ceará revogá-la, no todo ou em parte, por razões de interesse público derivadas de fato(s) superveniente(s) comprovado(s) ou anulá-la por ilegalidade, de ofício ou por provocação, mediante ato escrito e fundamentado, disponibilizado no sistema para conhecimento dos participantes da licitação. O Tribunal de Justiça do Estado do Ceará poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura.

19.2 Iniciada a etapa de lances, não caberá desistência da proposta, salvo por motivo justo decorrente de fato superveniente e aceito pelo(a) pregoeiro(a).

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

19.4 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.

19.5 O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará a imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato ou do pedido de compra, sem prejuízo das demais sanções cabíveis.

19.6 É facultado à(ao) Pregoeira(o) ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório, vedada a inclusão posterior de documentos que deveriam constar obrigatoriamente na proposta e na documentação de habilitação.

19.7 Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo(a) Pregoeiro(a), sob pena de desclassificação/inabilitação.

19.8 O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

19.9 As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento ou, ainda, mediante publicação no Diário da Justiça do Estado do Ceará.

19.10 Na contagem dos prazos estabelecidos neste Edital, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. Os prazos estabelecidos neste edital se iniciam e se vencem somente em dia de expediente no Tribunal de Justiça do Estado do Ceará.

19.11 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo prevalecerão as deste Edital.

19.12 A participação do licitante nesta licitação implica em aceitação de todos os termos deste Edital, e a inobservância de qualquer dos itens descritos nele é de total responsabilidade dos participantes.

19.13 Qualquer informação fornecida por telefone não terá caráter formal.

19.14 A existência de preços registrados não obriga o Poder Judiciário Estadual a firmar as contratações nas quantidades estimadas no Anexo 1 deste Edital, ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurada ao beneficiário do Registro, a preferência de contratação em igualdade de condições.

19.15 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será o de Fortaleza, Capital do Estado do Ceará, considerado aquele a que está vinculado o Pregoeiro.

19.16 É vedado ao servidor dos órgãos e entidades da Administração Pública Estadual, inclusive Fundações instituídas e/ou mantidas pelo Poder Público, participar como licitante, direta ou indiretamente, por si ou por interposta pessoa, dos procedimentos licitatórios disciplinados pela Lei n. 10.880/1983.

19.17 De acordo com a Resolução do CNJ n. 7, de 18.10.2005, e suas alterações, constitui prática de nepotismo a contratação, em casos excepcionais de dispensa ou inexigibilidade de licitação, de pessoa jurídica da qual sejam sócios cônjuges, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, ou servidor investido em cargo de direção e de assessoramento.

19.17.1 A vedação se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a

desincompatibilização.

19.17.2 A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo tribunal, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório.

19.17.3 É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal contratante.

19.18 Toda a documentação apresentada fará parte dos autos da licitação e não será devolvida ao licitante, ainda que se trate de originais.

19.19 Havendo divergência, exclusivamente quanto às especificações da descrição dos itens na descrição do sistema "*licitacoes-e*" do Banco do Brasil, Minuta de Contrato e outros, prevalecerão as descritas no Termo de Referência.

19.20 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 despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

19.21 Os casos omissos e não previstos neste Edital serão resolvidos pelo(a) Pregoeiro(a) do TJCE, nos termos da Legislação pertinente.

Fortaleza/CE, 06 de junho de 2024.

Sérgio Mendes de Oliveira Filho
SECRETÁRIO GERAL ADMINISTRATIVO DO TJCE

Denise Maria Norões Olsen
SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO DO TJCE

Aprovado:

Cristiano Batista da Silva
CONSULTOR JURÍDICO DA PRESIDÊNCIA DO TJCE

ANEXO 1 DO EDITAL – TERMO DE REFERÊNCIA

ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Termo de Referência – TR

CÓDIGO PAC 2024: TJCESETIN_2024_0031

AQSETIN2022020 - Soluções de Segurança – Firewall grande porte

1 OBJETO DA CONTRATAÇÃO

1.1 Esta contratação tem como objeto aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção pelo prazo de 60 (sessenta) meses; incluindo serviços de instalação, treinamento e demais especificações e características consignados neste Termo de Referência.

1.2 Quantitativo

Id	Bem/Serviço	Model/Part Number	Qtd.
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1

6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2
8	Implantação da solução de Firewall	---	1
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	---	1
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	---	1
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	---	1

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Motivação

2.1.1 Como o prazo de garantia/suporte/subscrições dos hardware e software adquiridos por meio do CT Nº 17/2018 expirarão em 2023, e considerando o aumento dos riscos variados de falha, à medida que os equipamentos envelhecem, e as Resoluções e Portarias acima citadas, faz-se necessário uma "Aquisição de solução de plataforma de segurança em cluster de firewalls" para atender a atual demanda, continuar a oferecer os serviços já citados acima, bem como, as novas necessidades tecnológicas, propiciando ganhos na segurança, estabilidade, disponibilidade e desempenho dos Sistemas Administrativos e Judiciais que utilizam a solução atual.

2.2 Resultados a serem alcançados com a contratação

2.2.1 Manutenção e controle do tráfego de rede;

2.2.2 Filtrar o conteúdo da Web:

2.2.3 Garantir que apenas navegadores web e clientes de e-mail suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.

2.2.4 Desinstalar ou desabilitar plug-ins ou aplicações add-on não autorizados para navegadores web e clientes de e-mail.

2.2.5 Utilizar filtros de URL baseados em rede de forma a limitar a possibilidade de sistemas se conectarem a websites não aprovados pela organização. Tais filtros devem ser impostos a todos os sistemas da organização, quer se encontrem dentro do espaço físico da organização, quer não.

2.2.6 Subscrever serviços de categorização de URLs de forma a garantir que o filtro

esteja atualizado com base nas mais recentes definições de categorias de sítios eletrônicos disponíveis. Sites não categorizados devem ser bloqueados por padrão.

2.2.7 Realizar registros de log de todas as requisições a URLs a partir de cada um dos sistemas da organização, quer nas dependências corporativas, quer em dispositivos móveis, de forma a identificar potenciais atividades maliciosas e auxiliar operadores de incidentes com a identificação de sistemas potencialmente comprometidos.

2.2.8 Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.

2.2.9 Prevenção da rede interna contra ameaças cibernéticas digitais;

2.2.10 Análise preventiva a incidentes de segurança: prevenção, detecção e resposta a incidentes baseadas nos eventos gerados pelo firewall;

2.2.11 Coleta e tratamento de dados relacionados a segurança;

2.2.12 Filtrar os dados;

2.2.13 Estabelecimento de canal de comunicação seguro através da VPN;

2.2.14 Aumento da confidencialidade, integridade e disponibilidade das informações do Poder Judiciário do Estado do Ceará;

2.2.15 Aumento da proteção da rede interna contra possíveis tentativas de acesso indevido;

2.2.16 Implementação de mecanismos de proteção, prevenção de intrusão;

2.2.17 Implementação de regras de segurança, além de proteção específica em nível de aplicações como correio eletrônico, servidores WEB;

2.2.18 Melhoria da qualidade dos serviços, da proteção das informações da instituição e da produtividade dos usuários; e

2.2.19 Capacitação e qualificação da equipe de TIC do Poder Judiciário do Estado do Ceará.

2.2.20 Manter a estabilidade, confiabilidade e proteção do tráfego de perímetro e da borda de acesso à Internet, através da renovação da solução atual que está em pleno funcionado e das expansões de segurança pretendidas;

2.2.21 Introduzir o conceito de Zero Trust na arquitetura de segurança do TJCE, permitindo que o Tribunal esteja atualizado com as melhores práticas e referências do mercado no quesito segurança da informação.

2.2.22 Além disso, a contratação oferece recursos para aperfeiçoar o monitoramento, controle, penalização e bloqueio de bots (robôs) que utilizam recursos em excesso da infraestrutura de TI e aplicações do TJCE na Internet, muitas vezes até causando

depreciação da performance dos sistemas e causando indisponibilidade nos serviços;

2.2.23 Prevenir, detectar e responder a incidentes baseadas nos eventos gerados pelo firewall;

2.2.24 Localizar anomalias dentro do ambiente com o uso de inteligência artificial;

2.2.25 Dispor de equipamentos e soluções com novas tecnologias e recursos;

2.2.26 Prover alta disponibilidade nos equipamentos e mecanismos que são a base para proteção contra-ataques cibernéticos dentro da infraestrutura do TJCE;

2.2.27 Garantir o nível de suporte técnico necessário para atender um ambiente corporativo complexo e robusto;

2.2.28 Aperfeiçoar a detecção e respostas a ameaças cibernéticas no ambiente do TJCE;

2.2.29 Suporte a solução a ser adquirida;

2.2.30 Obter suporte adequado do fabricante quando da necessidade de aperfeiçoamento, melhores práticas, dúvidas de utilização e resolução de problemas.

2.3 Referência aos Estudos Técnicos Preliminares

2.3.1 Os documentos que resultaram dos Estudos Técnicos Preliminares desta contratação seguem acostados nos respectivos autos do processo Administrativo que trata da demanda exposta nesse Termo.

2.4 Alinhamento estratégico

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da Setin
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

ID	INICIATIVA ELENCADA NO PDTIC (2023-2024)
N23005	Soluções de Segurança – Firewall grande porte: ampliação/renovação

2.5 Critérios Ambientais

2.5.1 A contratada deverá providenciar o recolhimento e o adequado descarte de produto(s) e material(is) inservível(is) originário(s) da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA n° 01, de 18/03/2010, da Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA n° 416, de 30/09/2009, e legislação correlata.

2.5.2 A contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 11º da Lei n.º 14.133/21.

2.5.3 Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

2.5.4 Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

2.5.5 Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva ROHS (*restriction of certain hazardous substances*), tais como mercúrio (hg), chumbo (pb), cromo hexavalente (cr(vi)), cádmio (cd), bifenil-polibromados (pbbs), éteres difenil-polibromados (pbdes).

2.5.6 Os serviços prestados e os bens fornecidos pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela Contratante.

2.6 Natureza do Objeto

2.6.1 A natureza do objeto a ser licitado é comum de acordo com o art. 6°, da Lei 14.133, de 2021 c/c art. 3º do Decreto nº 10.024/2019 que considera bens e serviços comuns, com fornecimento de equipamento, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações reconhecidas e usuais do mercado.

2.7 Natureza do Serviço, se continuado ou não

2.7.1 Não se trata de serviço contínuo, uma vez que o objeto da contratação compreende o fornecimento de equipamentos, acessórios e serviços de instalação e treinamento, executados de única vez, com vistas à capacitação, implantação, instalação e configuração da solução adquirida.

2.8 Justificativa para Adoção do Pregão

2.8.1 A modalidade da licitação sugerida é o Pregão Eletrônico, em conformidade com a Lei 14.133/21, tendo em vista o objeto se tratar de bem e serviço comum, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;

2.8.2 A contratação da solução ora pretendida é oferecida por diversos fornecedores no mercado de TIC. Assim, trata-se de serviço comum pois é fácil encontrar empresas no mercado que realizam o fornecimento de equipamentos e executam serviços de manutenção, suporte e garantia da solução pretendida. Devido à alta demanda por esses serviços, há uma ampla oferta de fornecedores com diferentes níveis de expertise e qualidade e, portanto, licitação via Pregão, em sua forma eletrônica, pelo tipo menor preço, e modo de disputa aberto e fechado.

2.9 Justificativa para Aplicação do Direito de Preferência (Lei complementar nº 123/06 e Lei nº 8.248/91)

2.9.1 Nos termos do art. 48, III da Lei Complementar n. 123, de 2006 (atualizada pela LC n. 147/2014), a Administração deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte. Por essa razão, parcela de até 25% (vinte e cinco por cento) dos quantitativos divisíveis deverão ser destinados exclusivamente a ME/EPP/COOP beneficiadas pela LC n. 123/2006. Essas "cotas reservadas" deverão ser definidas em função de cada item separadamente ou, nas licitações por preço global, em função do valor estimado para o grupo ou o lote da licitação que deve ser considerado como um único item (art. 9º, inciso I do Decreto n. 8.538, de 2015).

2.9.2 In casu, a licitação que se pretende deverá ocorrer pelo menor preço de cada item e do lote - previamente ao menor preço de cada item. Contudo, todos os itens se trata de serviços e equipamentos em sua totalidade, sendo 7 (sete) itens, não havendo, desta forma, como fazê-lo divisível sem desnaturá-lo.

2.9.3 A divisão não se torna possível seja pelo fato de tratar-se de item unitário, qual seja a contratação de serviço técnico profissional pelo período de 60 (sessenta) meses, seja pela indivisibilidade técnica da solução de proteção para acessos remotos.

2.9.4 Para tanto, o art. 10, incisos I, II e IV do Decreto nº 8.538, de 2015 excepciona algumas hipóteses, quais sejam: I - não houver o mínimo de três fornecedores competitivos enquadrados como microempresas [...] capazes de cumprir as exigências estabelecidas no instrumento convocatório; II - o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado, justificadamente; (...) IV - o tratamento diferenciado e simplificado não for capaz de alcançar, justificadamente, pelo menos um dos objetivos previstos no art. 1º. (grifo nosso)

2.9.5 No caso aqui exposto, com toda a contextualização elaborada até então, fica evidente de que o inciso II se amolda à situação ora posta, já vez que por se tratar de solução e serviços não divisíveis, não caberia particionar a entrega dos itens do lote entre fornecedores distintos.

2.9.6 Considera-se "não vantajosa a contratação" quando: I - resultar em preço superior ao valor estabelecido como referência; ou II - a natureza do bem, serviço ou obra for incompatível com a aplicação do benefício (Decreto nº 8.538, de 2015, art. 10, parágrafo único). (grifo nosso)

2.9.7 Diante do explanado, conclui-se que não há óbice quanto à aplicação da Lei Complementar 123/2006. Entretanto não é possível a divisão ou fragmentação dos itens em partes e nem aplicação do benefício da exclusividade para que ocorra a participação para ME/EPP, ante da impossibilidade da divisão técnica dos itens, conforme explanação apresentada neste Termo de Referência.

2.10 Da Subcontratação, Cisão ou Incorporação

2.10.1 Não será permitida a subcontratação total ou parcial do objeto.

2.10.2 Não será admissível a fusão, cisão ou incorporação da CONTRATADA.

3 DESCRIÇÃO DA SOLUÇÃO

3.1 Aquisição de solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, no modelo 24x7, pelo prazo de 60 (sessenta) meses; incluindo

serviços de instalação e treinamento.

3.2 A solução deve ser composta por dois equipamentos (appliances) que funcionam em cluster, especificamente projetados para atuar como Next Generation Firewall, com hardware e software fornecidos pelo mesmo fabricante.

3.3 Cada equipamento (appliance) integrante da solução de alta disponibilidade deve possuir licença ativada para suportar, de maneira simultânea e integrada, as seguintes funcionalidades: firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL, controle de transferência de arquivos, roteamento estático e dinâmico, NAT e com garantia durante 60 (sessenta) meses. Devem ser as **CARACTERÍSTICAS GERAIS do ANEXO I – ESPECIFICAÇÕES TÉCNICAS**.

3.4 A solução de gerenciamento centralizado deverá ser constituída de, no mínimo, um "appliance virtual", que é uma solução de software baseada em máquina virtual, seguindo os padrões estabelecidos pelo DMTF (Distributed Management Task Force). Alternativamente, poderá ser utilizado um sistema operacional desenvolvido pelo fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual. A instalação da solução de gerenciamento ocorrerá em um ambiente de virtualização e hardware pertencente ao TJCE.

3.5 É obrigatório que todos os equipamentos e seus componentes sejam novos, sem uso prévio, entregues em perfeitas condições de funcionamento e sem quaisquer sinais de danos físicos, tais como marcas, amassados, arranhões ou outras imperfeições. Além disso, devem ser acondicionados em suas embalagens originais.

3.6 Equipamentos que estejam no fim de sua vida útil ou não recebam mais suporte não serão aceitos.

3.7 Devido à complexidade das soluções de segurança, faz-se necessário manter um suporte técnico especializado, 24x7, com o objetivo de poder acionar um suporte técnico, obter recomendações de melhores práticas e assessoramento para o funcionamento da plataforma de solução de segurança.

3.8 Além disso, a garantia é fundamental para manter contratos de substituição de peças e equipamentos durante a vigência do contrato. Com o objetivo de garantir a continuidade dos serviços e a estabilidade do ambiente, a contratada deverá fornecer um novo hardware, que seja equivalente ou superior, para ser utilizado em situações de falha de equipamento, falha de fabricação, degradação dos serviços ou qualquer outro tipo de problema com a solução. Essa disponibilidade de hardware adicional é crucial para assegurar que o ambiente não seja interrompido ou degradado por tempo indeterminado. A contratada deve estar preparada para lidar

prontamente com qualquer eventualidade, minimizando os efeitos adversos sobre o funcionamento do equipamento. A capacidade de resposta rápida e eficiente nessas situações é essencial para manter a integridade e a confiabilidade do ambiente do tribunal, garantindo que as atividades judiciais e administrativas possam ser conduzidas sem interrupções significativas.

4 ESPECIFICAÇÃO TÉCNICA

4.1 Conforme consta no **ANEXO I**.

5 MODELO DE EXECUÇÃO DO OBJETO

5.1 Metodologia de Trabalho

Etapa/Fase/Item	Prazo / Condição
Reunião de alinhamento	Em até 5 (cinco) dias úteis após a data de assinatura do contrato.
Entrega do hardware	Em até 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.
Instalação, configuração e testes da solução	Em até 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.
Operação assistida	Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na tabela do item 1.2, com duração de 20 dias úteis, podendo ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços até que sejam sanadas para o atendimento dos requisitos técnicos.
Treinamento	Está condicionada à solicitação prévia, via emissão de ordem de serviço por parte da Contratante, em data a ser previamente acordada com o TJCE.
Documentação	Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço.
Período de suporte, monitoramento e garantia da solução de TI	60 (sessenta) meses após a emissão do Termo de Recebimento Definitivo.
Regime para atendimento da garantia on-site	NBD - Next Business Day (próximo dia útil) em atendimento no regime 24x7 (24 horas por dia, 7 dias na semana)

Etapa	Método
Entrega do Objeto	**01 (hum) Appliance de Firewall deverá ser entregue**: TJCE – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325, prédio ANEXO – Centro de Documentação e Informática (CDI) – Secretaria de Tecnologia da Informação/Departamento de Infraestrutura de TI. **01 (hum) Appliance de Firewall deverá ser entregue**: Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza - CE, 60811-690.Deverá ser conferido as quantidades por item.
Recebimento Provisório e Recebimento Definitivo	Quando da entrega do objeto do contrato, os equipamentos serão avaliados quanto as suas características técnicas, a fim de se verificar a conformidade com àquelas exigidas no Termo de Referência. Será também avaliado o tempo de fornecimento da solução dentro dos prazos especificados, que no caso da entrega do objeto, é de até 30 (trinta) dias corridos contados da data de emissão da Ordem de Fornecimento de Bens. O recebimento definitivo da solução de TI fornecida ocorrerá após recebimento e conclusão da etapa de "Instalação, configuração e testes da solução", por parte da Contratante, da conformidade do produto ofertado quanto às exigências contidas no Termo de Referência em até 10 (dez) dias corridos, contados da data de emissão do Termo de Recebimento Provisório.
Durante a Garantia	Durante a prestação da garantia, será avaliado o cumprimento dos prazos de solução dos chamados e a conformidade técnica dos equipamentos substituídos.

5.2 A execução do objeto deve incluir as fases de planejamento, instalação, configuração, migração tecnológica, elaboração de documentação técnica e operação assistida. Tais fases devem observar as seguintes condições:

5.2.1 Condições Gerais

5.2.1.1 A CONTRATADA é responsável por realizar as seguintes atividades, em conformidade com as especificações técnicas de cada item, apresentadas e aprovadas previamente pelo TJCE:

5.2.1.1.1 Planejamento, instalação, configuração e migração tecnológica.

5.2.1.1.2 Elaboração de documentação técnica.

5.2.1.1.3 Operação assistida dos serviços.

5.2.1.2 Estas atividades também abrangem o levantamento da solução atualmente em uso no Tribunal e a migração das configurações existentes para o ambiente proposto.

5.2.1.3 Desde o início das atividades referentes à fase de planejamento até o recebimento definitivo de cada item de serviço, a CONTRATADA deve alocar profissionais com experiência comprovada na tecnologia dos produtos para cada um dos serviços.

5.2.1.4 Da mesma maneira, a CONTRATADA deve manter profissional com papel de gerente de projeto para realização das atividades de planejamento, interlocução, elaboração de cronograma e entrega de documentação técnica associada à fase.

5.2.2 Etapas

5.2.2.1 Os Serviços Gerenciados de Segurança devem ser entregues em etapas:

5.2.2.1.1 Reunião de alinhamento

5.2.2.1.2 Entrega do hardware

5.2.2.1.3 Instalação, configuração e testes das soluções

5.2.2.1.4 Operação assistida

5.2.2.1.5 Treinamento

5.2.2.1.6 Documentação

5.2.3 Reunião de alinhamento

5.2.3.1 Em até 5 (cinco) dias úteis após a data de assinatura do contrato, deverá ser realizada reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e Anexos, bem como o planejamento e definições de roteiro de suporte técnico dedicado, e esclarecer possíveis dúvidas acerca da execução dos serviços.

5.2.3.2 O Plano de Implantação deverá ser alinhado na reunião de kick-off, juntamente com a equipe técnica da SETIN.

5.2.3.3 Deverão participar dessa reunião, no mínimo, os fiscais do contrato, o Preposto da Contratada e demais intervenientes necessários. Caso a contratante entenda que seja necessária a presença do fabricante, o mesmo deverá estar presente na call de Kick-off.

5.2.3.4 A reunião deverá ocorrer no TJCE ou por vídeo conferência, de preferência, antes do início da execução dos serviços / entrega dos bens, em data e horário a ser agendada pelos fiscais do contrato.

5.2.3.5 Nessa reunião, a Contratada deverá apresentar oficialmente seu Preposto, além da equipe técnica responsável pelo atendimento do serviço especializado e suas respectivas qualificações técnicas.

5.2.3.6 Será realizada, na reunião, o alinhamento dos aspectos principais para o Plano de Implantação que deverá ser entregue pela Contratada, idealizada por ambas as partes.

5.2.3.7 A Contratada deverá apresentar um número de telefone que possibilite ligações para a central de suporte, portal/url e endereço de e-mail para fins de abertura, acompanhamento de chamados e resolução de dúvidas sobre a Solução;

5.2.3.8 Os profissionais indicados pela Contratada deverão efetivamente atender os serviços objeto do contrato, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo TJCE.

5.2.3.9 A Contratada cumprirá as instruções complementares do TJCE quanto à execução e horário de realização do serviço, permanência e circulação de seu(s) técnico(s) nas dependências do TJCE.

5.2.4 Entrega do hardware

5.2.4.1 Após a assinatura do contrato, os fiscais do contrato ficarão aptos a solicitar o primeiro empenho.

5.2.4.2 A entrega dos equipamentos deverá ocorrer em, no máximo, 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.

5.2.4.3 Os equipamentos e componentes serão entregues pela CONTRATADA em perfeitas condições de operação, salvo quando ocorrerem situações fora do controle da mesma, tais como: greves nos serviços de transportes, guerras e perturbações de caráter social, político ou econômico, devidamente comprovadas e formalmente aceitas pelo TJCE.

5.2.4.4 Os equipamentos e materiais deverão ser entregues acondicionados adequadamente, em caixa lacrada, de forma a resistir à armazenagem e permitir completa segurança durante o transporte.

5.2.4.5 A entrega deverá ocorrer no horário das 08:00 às 17:00, de segunda a sexta-feira, exceto nos feriados nos seguintes endereços:

5.2.4.5.1 **01 (hum) Appliance de Firewall deverá ser entregue:** TJCE – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325, prédio ANEXO – Centro de Documentação e Informática (CDI) – Secretaria de Tecnologia da Informação/Departamento de Infraestrutura de TI.

5.2.4.5.2 **01 (hum) Appliance de Firewall deverá ser entregue:** Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza – CE, 60811-690.

5.2.4.6 O não cumprimento do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada, implicará as sanções administrativas previstas neste termo de referência.

5.2.4.7 A CONTRATADA deverá informar ao TJCE a disponibilidade do produto para que sejam tomadas todas as providências necessárias ao início da execução do teste de recebimento definitivo, a ser efetuado.

5.2.4.8 Entende-se como recebimento definitivo dos produtos, aquele recebido funcionando e em perfeitas condições, com a devida instalação, quando esta estiver prevista nas especificações.

5.2.4.9 Por ocasião do recebimento definitivo dos produtos será assinado documento pertinente, que integrará o Contrato.

5.2.4.10 Juntamente a cada produto entregue deverão constar os respectivos manuais de instruções e demais literaturas técnicas pertinentes, bem como respectivas notas fiscais e/ou faturas.

5.2.4.11 Caberá à Contratada a responsabilidade pela entrega dos bens, com todas as despesas de transporte, frete e seguro correspondentes;

5.2.4.12 O material deverá ser entregue pela Contratada em perfeitas condições de operação;

5.2.4.13 Deverá ser entregue, juntamente com os bens adquiridos, as respectivas notas fiscais e/ou faturas.

5.2.4.14 Por ocasião do recebimento provisório/definitivo dos produtos, será assinado documento pertinente, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021.

5.2.4.15 Sendo necessário o pedido de prorrogação de prazo para entrega dos materiais, somente será conhecido por este Tribunal caso tal pleito seja devidamente fundamentado e protocolado de maneira virtual, juntamente com documentação probatória das alegações, no e-mail dos fiscais do contrato, em até 05 (cinco dias) antes de expirar o prazo inicialmente estabelecido.

5.2.4.16 A garantia dos equipamentos e o serviço de suporte técnico iniciarão após a emissão do Termo de Recebimento Definitivo.

5.2.4.17 Constatado defeito de fábrica do material, cabos e módulos, em sua utilização durante o prazo de garantia do produto, a Contratada deverá substituí-los por outros iguais ou superiores, no prazo de dez (10) dias úteis contados a partir da notificação efetuada pelo Contratante, sem qualquer ônus adicional.

5.2.4.18 A garantia on-site dos equipamentos deverá ser realizada nos Data Centers do Tribunal de Justiça.

5.2.5 Instalação, configuração e testes das soluções

5.2.5.1 A execução dos serviços de instalação, configuração e disponibilização dos licenciamentos deverá ocorrer em, no máximo 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.

5.2.5.2 A CONTRATADA deverá entregar, em até 02 (dois) dias úteis após a conclusão da instalação dos equipamentos, relatório de instalação que deverá conter: confirmação de todos os equipamentos e perfeito funcionamento do hardware, identificação de cada produto instalado (marca, modelo, versão, número de série, número da licença, etc.), nome, matrícula, data e assinatura do técnico responsável pela CONTRATADA e do técnico do TJCE.

5.2.5.3 A CONTRATADA deve ser responsável por prover os recursos necessários à instalação e configuração de equipamentos, sem ônus adicionais ao Tribunal, incluindo o fornecimento de cabos elétricos, cabos lógicos, adaptadores elétricos, parafusos, porcas, conectores, kits racks, tomadas e demais materiais necessários à instalação de equipamentos nos locais de prestação dos serviços, incluindo o fornecimento de transceivers/transceptores para a utilização de interfaces de fibra-óptica.

5.2.5.4 Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no local da instalação dos equipamentos, bem como pela retirada e entrega dos mesmos, de peças de reposição e componentes necessários, com todas as despesas de transporte, frete e seguros correspondentes.

5.2.5.5 Além dos recursos de infraestrutura supracitados, a CONTRATADA deve ser responsável pelo fornecimento de licenças de sistemas operacionais, quando necessários para o provimento dos softwares integrantes da solução proposta. Nesse contexto, incluem-se sistemas operacionais básicos, patches de atualização, softwares de aplicações, softwares de bancos de dados, entre outros.

5.2.5.6 Ademais, os equipamentos e softwares necessários à prestação dos serviços devem estar cobertos por contratos de suporte técnico e garantia do fabricante durante o período de vigência de cada um dos itens de serviço.

5.2.5.7 Os softwares propostos e licenciados para a solução, excluindo aqueles a serem instalados em equipamentos para o provimento de serviços integrados, quando explicitamente permitidos, devem ser instalados em máquinas virtuais a serem providas pelo TJCE. Nesse contexto, incluem-se os softwares dimensionados para prover diretamente serviços da solução, bem como aqueles referentes à administração e monitoramento de equipamentos e serviços, que devem ser instalados em sua última versão estável e atualizada pelos respectivos fabricantes.

5.2.5.8 Ademais, os equipamentos e softwares devem ser integrados à base de usuários com privilégios administrativos do Microsoft Active Directory e RADIUS (Remote Authentication Dial-in User Service) da rede do Tribunal para concessão de perfis de

acesso às ferramentas implementadas. Nesse contexto, devem ser configurados 3 (três) perfis de acesso para os serviços: um perfil de leitura, consulta a informações, configurações e logs, para o acompanhamento da execução de serviços por parte da equipe técnica do TJCE; um perfil de controle total para a execução das atividades de administração e gerência remota da plataforma por parte da CONTRATADA; e um terceiro de controle total para a execução das atividades de administração e gerência da plataforma por parte da equipe técnica do TJCE, a ser utilizada somente em caso de grave emergência, como nos casos de sinistros que causem a indisponibilidade total dos serviços ou a indisponibilidade da CONTRATADA. Essas credenciais de acesso, para uso em caso de emergência, devem ser armazenadas em cofre do Tribunal, cujo procedimento de utilização deve ser acordado com a CONTRATADA em momento oportuno.

5.2.5.9 Todos os elementos instalados devem ser configurados para envio de logs para a solução de consolidação e correlacionamento de eventos do Tribunal, implantada em ambiente virtualizado, responsável pela coleta, processamento, normalização, armazenamento e correlação de eventos gerados pelos diversos servidores de rede e de aplicação. Dessa forma, as atividades de levantamento, desenvolvimento de conectores e implantação de casos de uso de correlacionamento da solução implantada deve fazer parte das etapas de implantação da solução.

5.2.5.10 Além disso, os equipamentos e softwares fornecidos devem ser configurados para enviar notificações e alarmes de performance e disponibilidades ao software de monitoramento adotado e implantado na infraestrutura do TJCE.

5.2.5.11 Faz parte da fase de instalação a interação com as equipes do TJCE para configuração das rotinas de backup da solução ofertada e da realização de testes de restore e de desligamento/religamento da solução.

5.2.5.12 Finalmente, todas as regras, configurações e serviços existentes na solução de segurança atualmente instalada no TJCE devem ser avaliadas e os elementos instalados devem ser configurados de forma a compatibilizar tudo com os ajustes necessários para melhoria e otimização, de forma a garantir nível de segurança igual ou superior.

5.2.5.13 O licenciamento de uso e a execução dos serviços de suporte técnico e garantia deverão ser iniciadas com base na data de recebimento definitivo dos seus respectivos equipamentos.

5.2.5.14 A garantia dos equipamentos e software terá vigência de 60 (sessenta) meses contados da data dos respectivos recebimentos definitivos e para os itens que

envolvem entrega de novos equipamentos.

5.2.6 Operação assistida

5.2.6.1 Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na tabela do item **1.2**.

5.2.6.2 A operação assistida deve ter a duração de 20 dias úteis, de modo a assegurar a execução de ações rápidas corretivas necessárias ao bom funcionamento dos serviços e reduzir riscos inerentes à migração tecnológica da plataforma atualmente existente.

5.2.6.3 As atividades de operação assistida devem ser realizadas obrigatoriamente com a presença de técnico capacitado, em horário comercial, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário comercial, sem qualquer ônus para o TJCE.

5.2.6.4 A duração das atividades de operação assistida pode ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços até que sejam sanadas para o atendimento dos requisitos técnicos.

5.2.6.5 O período de operação assistida deve englobar, entre outras, as seguintes atividades para cada um dos itens de serviço:

5.2.6.5.1 Monitoramento de funcionamento e da capacidade dos serviços, resolução de problemas (troubleshooting), análise da efetividade de regras e configurações, simulação de abertura de chamados, instalação de patches, execução/revisão de procedimentos de backup e restore de configurações, definição de casos de uso para correlacionar eventos, manutenção da documentação técnica e revisão de boletins e indicadores;

5.2.7 Treinamento

5.2.7.1 A prestação dos serviços relacionados ao item de Treinamento – está condicionada à solicitação prévia, por uma ordem de serviço, em data a ser previamente acordada com o TJCE.

5.2.7.2 A alteração dos prazos para início e término de uma Ordem de Serviço somente deve ser possível mediante apresentação tempestiva de justificativas plausíveis, a serem analisadas e devidamente aceitas pelo Tribunal.

5.2.8 Documentação

5.2.8.1 Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço,

contendo as seguintes informações:

5.2.8.1.1 Descrição dos serviços implantados, assim como os procedimentos de instalação e configuração;

5.2.8.1.2 Descrição da topologia física de equipamentos após a ativação dos serviços e o cenário de implantação e integração da rede;

5.2.8.1.3 Descrição de topologia lógica e detalhes de design de baixo nível (por exemplo, endereços IP, nomes de dispositivos, matriz de cabeamento, pesquisa do local, configuração específica do site/dispositivo);

5.2.8.1.4 Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

5.2.8.1.5 Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

5.2.8.1.6 Hardening/segurança do sistema;

5.2.8.1.7 Definição de responsabilidades;

5.2.8.1.8 Recursos de alta disponibilidade;

5.2.8.1.9 Scripts de operação, incluindo desligamento e ligamento, switch over, acionamento do equipamento de contingência, quando necessário;

5.2.8.1.10 Procedimentos para abertura e atendimento a chamados;

5.2.8.1.11 Procedimentos de recuperação de equipamentos;

5.2.8.1.12 Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

5.2.8.1.13 Rotinas periódicas configuradas;

5.2.8.1.14 Desenho dos racks onde estão instalados os equipamentos (bayface);

5.2.8.1.15 Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos)

5.2.8.1.16 Documentação das informações de configuração cadastradas.

5.3 Instrumentos de Solicitação do Serviço de Suporte Técnico e Monitoramento

5.3.1 Abertura em central de atendimento único para todos os serviços;

5.3.2 Serão utilizados os seguintes instrumentos formais de solicitação do(s) serviço(s):

5.3.2.1 Atendimento através de canal telefônico gratuito 0800 ou com custo de ligação local em Fortaleza/CE, 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.3.2.2 Chamado técnico através de site na Internet da CONTRATADA, 24x7 (vinte e quatro horas por dia, sete dias por semana), e/ou canal telefônico gratuito 0800 ou custo de ligação local para Fortaleza/CE;

5.3.3 No provimento deste serviço por meio de telefone (0800), a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

5.3.4 Para os atendimentos por meio de telefone (0800) ou de Call Center, o tempo máximo de espera deverá ser de até 03 (três) minutos.

5.3.5 No caso de a CONTRATADA optar pelo atendimento por Website, deverá ser possível que ao TJCE indique uma lista de produtos por meio de arquivo anexo ou diretamente na página, em um único registro. Neste caso, a data e hora do registro serão consideradas como horário da abertura do chamado para todos os produtos listados.

5.3.6 A CONTRATADA deverá permitir que o TJCE acompanhe o estado de chamados abertos no Centro de Assistência Técnica do fabricante por meio de site da Internet. O acesso ao Centro de Assistência Técnica deverá estar disponível durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, passível de penalidade em caso de descumprimento, conforme disposto no item **11** deste Termo de Referência.

5.3.7 O horário de abertura de chamado será determinado conforme abaixo:

5.3.7.1 Para chamados abertos pelos canais 0800 ou Call Center → o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional do TJCE informando do problema ocorrido. Caso a atendente não possa informar o número e chamado neste momento, a mesma deverá, obrigatoriamente, informar um número de protocolo que registre a data e hora da ligação realizada.

5.3.7.2 Para chamados abertos pelo canal Website → o horário da abertura do chamado será a data e hora do acesso ao Website para registro do problema ocorrido. No momento do registro, a página web deverá informar o número de chamado. Caso isso não seja possível, a mesma deverá informar um número de protocolo que registre a data e hora do acesso realizado.

5.3.8 O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA. O horário de abertura de chamado será determinado conforme descrito no subitem **5.3.7** deste Termo de Referência.

5.3.9 O horário de abertura do chamado demarcará o início da contagem do prazo de retorno, para os chamados estabelecidos como severidade 4, independente do retorno da CONTRATADA. O horário de abertura de chamado será determinado conforme descrito no subitem **5.3.7** deste Termo de Referência.

5.3.10 Não deverá haver qualquer limitação para o número de técnicos do TJCE autorizados a abrir chamados técnicos.

5.4 Local de Execução do Serviço

5.4.1 A execução dos serviços, assim como a instalação dos equipamentos deverá ocorrer nos seguintes endereços, após agendamento prévio com os fiscais do contrato:

5.4.1.1 **Tribunal de Justiça do Estado do Ceará**, situado na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325.

5.4.1.2 **Fórum Clóvis Beviláqua**, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza – CE, 60811-690.

5.5 Horário de Execução do Serviço

5.5.1 A prestação dos serviços presenciais de suporte técnico, instalação e configuração dos equipamentos de verão ocorre normalmente de segunda a sexta-feira, das 8h às 18h, a menos que haja um acordo prévio entre as partes. Em casos de execução de garantia, substituição de hardware ou emergências que exijam atendimento 24 horas por dia, 7 dias por semana, o serviço será disponibilizado mediante acordo prévio.

5.5.2 Os serviços serão solicitados mediante a abertura de um "chamado", efetuado por técnicos do Contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português – para o horário comercial – horário oficial de Brasília).

5.5.3 Para entrega, instalação e configuração dos equipamentos, deverá seguir agendamento prévio com os fiscais do contrato.

5.5.4 **Relatório de Instrumento de Medição de Resultados:** Relatório elaborado mensalmente pela Contratada e encaminhado via e-mail aos fiscais do contrato, contendo, no mínimo, as seguintes informações:

5.5.4.1 Contratante;

5.5.4.2 Número do Contrato;

5.5.4.3 Endereço;

5.5.4.4 Mês de Referência;

5.5.4.5 Data da realização;

5.5.4.6 Data de registro do chamado, início e fim do atendimento;

5.5.4.7 Fiscal técnico responsável;

5.5.4.8 Responsável técnico da Contratada;

5.5.5 A Contratante possui ampla liberdade de contestar os dados informados no Relatório de Instrumento de Medição de Resultados, podendo solicitar correções no mesmo, no prazo de 3 (três) dias úteis, caso identifique que as informações apresentadas estejam incorretas.

5.5.6 Após a análise e aprovação deste relatório, a Contratante deverá emitir o documento "Autorização para Faturamento", descrito no item 5.5.7 deste Termo de Referência.

5.5.7 Autorização para Faturamento: Autorização emitida pelo Fiscal Administrativo do Contrato ao Preposto da Contratada. Este documento contém a autorização para que a Contratada possa efetuar o faturamento.

5.6 Instrumento de Medição de Resultados – IMR

5.6.1 A prestação do Serviço Técnico executado terá sua qualidade medida por meio de Instrumento de Medição de Resultados – IMR.

5.6.2 Havendo qualquer interrupção ou mal funcionamento da solução, o TJCE efetuará abertura de chamado reportando todos os sintomas.

5.6.3 Serão considerados para efeitos de medição de resultados:

5.6.3.1 **Prazo de Atendimento:** Tempo decorrido entre a abertura do chamado técnico efetuado pelo TJCE na Central de Atendimento do Contratado e o efetivo início dos trabalhos de suporte.

5.6.3.2 **Prazo de Solução Definitiva:** Tempo decorrido entre a abertura do chamado técnico efetuado pela SETIN na Central de Atendimento do Contratado e a efetiva recolocação da solução em pleno estado de funcionamento.

5.6.4 A contagem do prazo de solução definitiva de cada chamado será a partir da abertura do chamado técnico na Central de Atendimento disponibilizado pelo Contratado, até o momento da comunicação da solução definitiva do problema e aceite pela SETIN.

5.6.5 As características do serviço IMR são as seguintes:

5.6.5.1 **Horário Comercial de Atendimento:** 08h às 18h, de segunda a sexta-feira;

5.6.5.2 **Tempo de solução**: varia de acordo com a severidade;

5.6.5.3 O prazo de solução poderá ser prorrogado, de acordo com as tratativas do atendimento, mediante aprovação prévia dos fiscais do contrato;

5.6.5.4 Em casos comprovados em que a resolução da solução dependa exclusivamente do fabricante, o prazo poderá ser prorrogado, conforme definido entre os fiscais e a empresa contratada;

5.6.5.5 **Intervalo de cobertura**: 24 x 7 (24 horas por dia, 7 dias por semana)

5.6.5.6 **Suporte a distância/remoto**: Assistência remota para solução de problemas comuns de suporte.

5.6.5.7 Todo e qualquer procedimento de atualização remota deve ser programado, previamente, entre a CONTRATADA e os fiscais do contrato, através de e-mail.

5.7 Indicadores de Instrumento de Medição de Resultados – IMR

5.7.1 Os Indicadores do Instrumento de Medição de Resultados (IMR) serão elencados para os serviços de suporte técnico da solução.

5.7.2 Os serviços serão medidos, controlados e acompanhados pela Contratante durante o período de vigência do contrato, assim como a definição do Instrumento de Medição do Resultado (IMR), com os acordos de níveis de serviço desejado e suas respectivas notificações ou penalidades.

5.7.3 O principal elemento para medir a qualidade e a eficácia dos serviços prestados pela Contratada será o IMR. Com relação a esse item, serão considerados os seguintes aspectos:

5.7.3.1 O IMR será aplicado a todos os serviços prestados pela Contratada indicados nesse tópico e não por amostragem.

5.7.3.2 Objetivando a qualidade, a Contratada deverá estabelecer procedimentos e condições que permitam a melhoria contínua dos serviços prestados.

5.7.3.3 As medições dos indicadores de nível de serviço serão aferidas pelos fiscais do contrato.

5.7.3.4 O não cumprimento de um ou mais indicadores do IMR ocasionará a aplicação de notificação ou penalidades à Contratada previstas em contrato.

5.7.3.5 A Contratante poderá avaliar as justificativas fundamentadas apresentadas pela Contratada para não aplicação das notificações ou penalidades.

5.7.4 Ao abrir um chamado relativo ao serviço de suporte técnico, o Contratante poderá classificá-lo em 4 (quatro) níveis de severidade:

5.7.4.1 **Severidade 1:** quando ocorre a paralisação dos sistemas objeto desta contratação, configurando-se como situação de emergência.

5.7.4.2 **Severidade 2:** quando se verifica uma grave perda de funcionalidades em programas ou sistemas do TJCE, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço;

5.7.4.3 **Severidade 3:** quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas do TJCE, causando apenas inconveniências para a devida prestação dos serviços pelo TJCE;

5.7.4.4 **Severidade 4:** quando se verifica como necessária a prestação de suporte local proativo para orientação e apoio às melhores práticas para análise do ambiente, execução de implementações visando melhorias na arquitetura, integrações, capacidade, desempenho e elaboração de relatórios executivos, gerenciais e operacionais, sem que haja indisponibilidade e/ou perda de funcionalidades dos sistemas do TJCE, incluindo a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas.

5.7.5 A Contratada deverá respeitar os seguintes Instrumentos de Medição de Resultados para o suporte técnico da solução, consoante cada indicador do IMR:

Prazo máximo para solução definitiva, ou apresentação de solução de contorno.	
Chamados de Severidade 1	Até 4 Horas, contados a partir do registro do chamado.
Comprometimento para início do atendimento e resposta	
Chamados de Severidade 2	Até 30 Minutos, contados a partir do registro do chamado.
Chamados de Severidade 3	Até 2 Horas, contados a partir do registro do chamado.
Chamados de Severidade 4	Até 4 Horas, contados a partir do registro do

	chamado.
Ferramentas de Suporte	
Últimos Hot Fixes e Service Packs	Sim
Grandes Upgrades e Melhorias	Sim
Acesso a fóruns de produtos da Fabricante	Acesso Total
Acesso a Base de Conhecimento de Suporte On-Line	Especialista
Suporte de Hardware	
Determinação de RMA – Autorização para devolução de material	Parceiro
Método de envio RMA – Autorização para devolução de material	Próximo vôo / Express Delivery (quando aplicável) ou Envio no Mesmo Dia Útil.

5.7.6 O nível de severidade será atribuído pelo TJCE no momento da abertura do chamado.

5.7.7 Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.

5.7.8 Toda e qualquer despesa decorrente do suporte remoto ou “on site” desses atendimentos serão de responsabilidade da CONTRATADA.

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

5.7.10 Em quaisquer casos e quando necessário, a CONTRATADA deverá enviar informações, para o e-mail dos fiscais técnicos, sobre as correções a serem aplicadas.

5.7.11 Caso não haja manifestação da CONTRATADA dentro do prazo definido no item **5.7.5** ou caso o Fiscal do Contrato entenda ser improcedente a justificativa apresentada, será iniciado processo de sugestão de aplicação de penalidades previstas, conforme o IMR transgredido.

5.7.12 Após a conclusão do suporte, a Contratada comunicará o fato aos fiscais do contrato e solicitará autorização para o fechamento do chamado. Caso o mesmo não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efeti-

vamente solucionado pela Contratada. Nesse caso os fiscais do contrato informarão as pendências relativas ao chamado aberto.

5.7.13 Sempre que houver quebra dos IMR, o(s) fiscal(is) técnico(s) emitirá(ão) notificação a Contratada, ou seu preposto, que terá o prazo de, no máximo, 05 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

5.7.14 Caso não sejam observados os prazos para atendimento previstos, ou ainda se a justificativa apresentada não for aceita pelos fiscais responsáveis do Contrato, a Contratada estará sujeita a multas/glosas, calculadas sobre o valor descrito mensal do contrato.

5.7.15 A solução deverá realizar upload de logs (diagnósticos) pelo sistema, para o fabricante, de forma a permitir diagnósticos mais eficazes.

5.7.16 Ao final de cada mês, a CONTRATANTE avaliará o cumprimento, pela Contratada, dos IMR, conforme subitem **5.7.5** deste Termo de Referência.

5.7.17 Caso haja descumprimento dos IMR, por problemas alheios à CONTRATANTE, e se as justificativas apresentadas pela Contratada forem consideradas insuficientes pela fiscalização, será aplicado desconto à fatura mensal do serviço de atualização e suporte técnico das subscrições, conforme o disposto abaixo:

SEVERIDADE	DESCRIÇÃO	PENALIDADE
1	Prazo de Solução	Glosa de 20% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 5% sobre o valor da fatura mensal do serviço a cada dia de atraso.
2	Prazo de Solução	Glosa de 10% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 2,5% sobre o valor da fatura mensal do serviço a cada dia de atraso.
3	Prazo de Solução	Glosa de 5% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 1% sobre o valor da fatura mensal do serviço a cada 2(dois) dias de atraso.
4	Prazo de Solução	Glosa de 2,5% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de

		0,5% sobre o valor da fatura mensal do serviço a cada 3(três) dias de atraso.

5.7.18 A aplicação das glosas acima descritas estará restrita ao máximo de 02 (duas) ocorrências (chamados técnicos), podendo ser acumulado os valores de multa quando alterado a severidade pelos fiscais do contrato, durante a vigência do contrato.

5.7.19 A CONTRATADA ficará sujeita às penalidades previstas no item **5.7.17**, sem prejuízo das Sanções Administrativas constante nesse Termo de Referência.

5.7.20 O atraso no prazo de solução, de qualquer severidade disposta no item **5.7.5**, superior a 25 (vinte e cinco) dias ou após 02 (duas) ocorrências (chamados técnicos) - item **5.7.18** – autoriza a Administração aplicar as sanções previstas no item **11**, e se for o caso, promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem o inciso I do art. 137 da Lei n. 14.133 de 2021.

5.7.21 As penalidades previstas neste Termo de Referência não excluem aquelas dispostas na Lei nº 14.133/21 Art. 156 e 162.

5.8 Das considerações acerca das soluções de contorno

5.8.1 Considerando que a solução das ocorrências de substituição de equipamentos, pela sua natureza, pode envolver atividades relacionadas importação de procedimentos alfandegários, admite-se para todos os casos a adoção de solução de contorno, respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível. Neste caso, a partir do encerramento do chamado original com a disponibilização da solução de contorno, deverá ser imediatamente aberta uma nova ocorrência para provimento da solução definitiva, na qual deverá constar, obrigatoriamente, um novo campo contendo o número do chamado original (encerrado com a solução de contorno, mais Severidade).

5.8.2 A solução de contorno não deverá utilizar-se de tempo superior a 50% (cinquenta por cento) do prazo definido para a severidade do qual o chamado está sendo executado.

5.9 O prazo máximo para disponibilização da solução definitiva será:

Prazos para solução definitiva (a partir do encerramento do chamado original, com a

disponibilização da solução de contorno)	
Severidade Informada	**Tempo para solução**
1	15 dias corridos
2	20 dias corridos
3	30 dias corridos
4	Conforme agendamento

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

5.9.2 Em caso de impossibilidade da disponibilização de solução de contorno ou definitiva, dentro dos prazos estabelecidos, a CONTRATADA deverá, ainda dentro destes prazos, emitir um parecer com previsão de novo prazo, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a abertura do respectivo chamado.

5.9.3 Após avaliação deste parecer inicial, o TJCE decidirá sobre a periodicidade da emissão de pareceres ou laudos posteriores, até o fechamento final do atendimento, sem prejuízo da aplicação das penalidades previstas pelo descumprimento dos prazos estabelecidos.

5.9.4 Em quaisquer casos e quando necessário, a CONTRATADA deverá enviar informações, para o e-mail dos fiscais do contrato, sobre as correções a serem aplicadas ou a própria.

5.9.5 Caso não haja manifestação da CONTRATADA dentro do prazo definido no item 5.9 ou caso os Fiscais do Contrato entendam ser improcedente a justificativa apresentada, será iniciado processo de sugestão de aplicação de penalidades previstas, conforme tabela do item **5.7.17**.

5.9.6 Após a conclusão do suporte, a CONTRATADA comunicará o fato aos Fiscais do contrato e solicitará autorização para o fechamento do chamado. Caso os mesmos não confirmem a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso os Fiscais do contrato informarão as pendências relativas ao chamado aberto.

5.9.7 Sempre que houver quebra dos IMR, os fiscais do contrato emitirão notificação à CONTRATADA, ou seu preposto, que terá o prazo de, no máximo, 05 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

5.9.8 Caso não sejam observados os prazos para atendimento previstos, ou ainda se a justificativa apresentada não for aceita pelos fiscais responsáveis do Contrato, a CONTRATADA estará sujeita a multas/glosas, calculadas sobre o valor descrito mensal do contrato.

5.9.9 A aplicação das glosas estará restrita ao máximo de 02 (duas) ocorrências (chamados técnicos), podendo ser acumulado os valores de glosas quando alterado a severidade pelo fiscal técnico, durante a vigência do contrato.

5.9.10 A CONTRATADA ficará sujeita às penalidades previstas, sem prejuízo das Sanções Administrativas constante nesse Termo de Referência.

5.9.11 O atraso no prazo de solução, de qualquer severidade disposta no item 5.7.4, superior a 25 (vinte e cinco) dias ou após 2 (duas) ocorrências (chamados técnicos) autoriza a Administração aplicar as sanções previstas no item **11**, e se for o caso, promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem o inciso I do art. 137 da Lei n.14.133/2021.

5.9.12 As penalidades previstas neste Termo de Referência não excluem aquelas dispostas na Lei nº 14.133/2021 Art. 162.

5.10 Monitoramento da Execução

5.10.1 Será efetuado pelos Fiscais Demandantes, Técnicos e Administrativos.

5.11 Qualidade e Recebimento

5.11.1 O processo de recebimento do objeto será regido conforme previsto no artigo 140, da Lei nº 14.133/21, e será realizado pelos fiscais do contrato. Acaso precise, pela Comissão de Recebimento de Bens do TJCE.

5.11.2 Por ocasião do recebimento provisório/definitivo dos produtos/serviços, será assinado documento pertinente, em conformidade com o estabelecido no 140, da Lei nº 14.133/21.

5.11.3 Forma de Recebimento Provisório – Equipamentos e serviços

5.11.3.1 Será considerado o recebimento provisório dos itens objeto desta contratação mediante a entrega destes ao Poder Judiciário Cearense.

5.11.3.2 Quando desta entrega, será realizado o recebimento provisório, para efeito de verificação da conformidade dos produtos com as especificações constantes deste Termo de Referência;

5.11.3.3 Os fiscais do contrato deverão, após a comprovação do perfeito funcionamento do serviço/material, emitir e assinar, em no máximo 5 (cinco) dias úteis, contados do primeiro dia útil posterior à entrega dos serviços/bens, o Termo de Recebimento Provisório.

5.11.3.4 Os serviços/bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias úteis, a contar da notificação do Contratante, às suas custas, sem prejuízo da aplicação das penalidades.

5.11.3.5 O Contratado deverá informar a SETIN a disponibilidade dos serviços, por meio do endereço eletrônico coordenadoria.seginfo@tjce.jus.br, endereçado aos fiscais do contrato, para que sejam tomadas todas as providências necessárias ao início dos trabalhos.

5.11.4 Os produtos deverão estar lacrados e não deverão apresentar quaisquer sinais de violação, marcas de quedas, umidades ou quaisquer outros sinais/características que demonstrem avarias, reservado ao Tribunal de Justiça o direito de recusar o recebimento.

5.11.4.1 Os fiscais do contrato e a Comissão de Recebimento de Bens Permanentes, caso esta precise atuar, deverão, após comprovado o perfeito funcionamento dos equipamentos e das adequações às especificações técnicas descritas no Termo de Referência, emitir e assinar, em no máximo 5 (cinco) dias úteis, contados do primeiro dia útil posterior à entrega dos mesmos, o Termo de Recebimento Provisório, devendo ser entregue à Contratada.

5.11.5 **Forma de recebimento definitivo – Equipamentos e serviços**

5.11.5.1 No recebimento e aceitação dos equipamentos, serão observadas as especificações contidas neste Termo de Referência e as disposições contidas no Artigos 140 da Lei 14.133/21 e Lei nº 10.520/02, e suas alterações.

5.11.5.2 Após a emissão da ordem de serviço à CONTRATADA, a mesma deverá iniciar, de imediato, a execução dos serviços de instalação e configuração, que deverá ser finalizado dentro do prazo de até 15 (quinze) dias corridos contados da data de emissão da ordem de serviço para a CONTRATADA.

5.11.5.3 As especificações serão avaliadas, também, por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e as disponíveis no site do fabricante.

5.11.5.4 A solução será recebida definitivamente pelos fiscais do contrato, em até 10 (dez) dias úteis após a instalação / ativação e configuração dos equipamentos / sistemas e entrega da solução em pleno funcionamento e operação, com a devida aprovação dos testes pelos fiscais do contrato da demanda.

5.11.5.5 As especificações serão avaliadas, também, por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e as disponíveis no site do fabricante.

5.11.5.6 Apresentado o Termo de Recebimento Definitivo e a Nota Fiscal Eletrônica de Venda – devidamente acompanhada dos documentos solicitados neste Termo de Referência, aos fiscais do contrato e à Comissão de Recebimento de Bens Permanentes, acaso esta precise atuar, devem estes, conjuntamente, atestá-la, encaminhando-a, com o Termo de Recebimento Definitivo, ao Fiscal Administrativo, que após proceder a devida análise no exercício das atribuições regulamentares previstas no § 3º, Art. 24, Seção III da Resolução 468/CNJ, também a atestará, encaminhando-a, posteriormente, ao departamento responsável ao pagamento, com as certidões cabíveis para o feito.

5.11.5.7 Se, a qualquer tempo, vier a ser constatado que o equipamento fora fornecido em desacordo com as especificações e, em decorrência desse fato, verificar qualquer tipo de dano ao equipamento no local em que está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da contratada.

5.11.5.8 A Contratada obrigar-se-á a efetuar a troca, às suas expensas, do equipamento que vier a ser recusado, não implicando na aceitação do mesmo o ato de recebimento.

5.11.5.9 Ocorrendo qualquer problema de fabricação, a Contratada terá o prazo de 10 (dez) dias úteis para proceder às correções a partir da notificação, adequações ou substituição do (s) produto (s) objeto deste ajuste.

5.11.5.10 Caso a correção dos problemas constatados não seja efetuada no período de até 10 (dez) dias úteis, contados a partir da data da primeira notificação, a Contratada

deverá trocar os equipamentos em até 48 horas e em definitivo, sem ônus para o TJCE;

5.11.5.11 Caso os equipamentos contratados não atendam ao especificado ou apresentem defeitos, serão considerados não entregues e a contagem do prazo de entrega não será interrompida devido à rejeição dos mesmos. Neste caso, a Contratada arcará com o (s) ônus decorrente (s) desse atraso, passível de penalidade, conforme disposto no item **11** deste Termo de Referência.

5.11.5.12 O aceite e o posterior pagamento dos equipamentos/serviços não eximem a licitante vencedora das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades.

5.11.6 Forma de recebimento definitivo Objeto – Suporte Técnico

5.11.6.1 A garantia da solução será de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo, e engloba os cabos e módulos objetos do presente no Termo de Referência, incluindo assistência corretiva, compreendendo a substituição de peças, componentes que apresentem defeito durante este período, sem qualquer ônus adicional para o TJCE, obrigando-se a Contratada a manter os materiais permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, assim como o pleno funcionamento dos software contratados.

5.11.6.2 Todos os custos referentes à coleta, transportes e devolução dos materiais, no período de garantia, são de responsabilidade da Contratada.

5.11.6.3 A garantia técnica compreende todas as funcionalidades dos materiais adquiridos, tanto as descritas neste Termo de Referência, quanto as contempladas nos manuais e demais documentos técnicos.

5.11.6.3.1 Será efetuada pela Contratada, sem ônus para o Contratante, a troca de todas e quaisquer partes, peças e equipamentos que se revelarem defeituosos, independentemente de causa ou do tipo de defeito.

5.11.6.3.2 Todas as peças e componentes substituídos deverão ser originais ou certificados pelo fabricante e sempre “novos e de primeiro uso”, não podendo ser recondicionados, com apresentação de documentos para tanto.

5.11.6.3.3 O serviço de garantia/suporte prestado deverá ser realizado no idioma português (Brasil).

5.11.6.3.4 Caso o equipamento, identificado pelo seu número de série, apresente o mesmo defeito recorrente após o segundo conserto, a Contratada deverá substituí-lo por outro idêntico ou superior, sem qualquer ônus para o TJCE.

5.11.6.3.5 Os parâmetros para abertura de chamado para Assistência Técnica estão contidos no item **5.7**.

5.12 Forma de avaliação da qualidade dos bens e/ou serviços entregues

5.12.1 Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, o TJCE, através dos fiscais do contrato, realizará, anualmente, a Avaliação de Desempenho, o que permitirá a adoção de eventuais ajustes no modelo de atendimento, conforme critérios abaixo, podendo ser criados outros que se fizerem necessários.

5.12.2 **Comunicação**: Avaliação qualitativa da comunicação do Contratado, como clareza na informação, formas de solicitações e questionamentos ao TJCE, educação e nível de formalidade no atendimento e tempo de resposta às solicitações.

5.12.3 **Confiabilidade**: Prestação correta (isenta de falhas e erros) do serviço/atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas.

5.12.4 **Organização**: Demonstração de planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

5.12.5 Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos conceitos abaixo:

5.12.6 Péssimo (de 0 a 4,9) / Regular (de 5 a 7,4) / Bom (de 7,5 a 8,9) / Ótimo (de 9 a 10).

5.12.7 Anualmente, a empresa contratada será informada do conceito médio obtido no período e registrado nos autos do contrato, resultado este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

6 Deveres e Responsabilidades da Contratante

6.1.1 Designar formalmente, na forma do art. 177, da Lei nº 14.133/21, representantes para gerenciar e exercer a fiscalização da execução do Contrato, independentemente do acompanhamento e controle exercido pela Contratada.

6.1.2 Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE;

6.1.3 Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. O mesmo deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados ou bens entregues e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços/entrega de bens, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

6.1.4 Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas;

6.1.5 Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com os termos do contrato assinado.

6.1.6 Proporcionar todas as condições e prestar as informações necessárias para que a Contratada possa cumprir com suas obrigações, dentro das normas e condições contratuais.

6.1.7 Prestar, por meio dos fiscais do contrato do Contrato, as informações e os esclarecimentos pertinentes aos serviços/bens avençados, que porventura venham a ser solicitados pela Contratada;

6.1.8 Informar à Contratada sobre atos que possam interferir direta ou indiretamente nos serviços prestados/entrega de bens;

6.1.9 Comunicar oficialmente à Contratada quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

6.1.10 Registrar e oficializar a Contratada sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

6.1.11 Rejeitar, no todo ou em parte, os serviços executados / a entrega de equipamentos que não atendam às especificações técnicas deste Termo de Referência.

6.1.12 Aprovar ou rejeitar, no todo ou em parte, os serviços executados / a entrega de equipamentos que não estiverem em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

6.1.13 Efetuar o pagamento devido pela prestação dos serviços executados / a entrega de equipamentos, desde que cumpridas todas as formalidades e exigências avençadas.

6.1.14 Aplicar as sanções previstas em contrato, assegurando à Contratada o contraditório e a ampla defesa.

6.1.15 Exigir, sempre que necessário, a apresentação da documentação pela CONTRATADA que comprove a manutenção das condições que ensejaram a sua contratação.

7 Deveres e Responsabilidades da Contratada

7.1.1 Manter atualizados seus dados cadastrais junto ao Tribunal de Justiça do Estado do Ceará.

7.1.2 Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela Contratada, sem ônus adicional a este Tribunal de Justiça.

7.1.3 Cumprir fielmente os Instrumentos de Medição de Resultados conforme itens **5.6**, **5.7** e demais especificações técnicas deste Termo de Referência.

7.1.4 Conceder acesso ao TJCE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do TJCE.

7.1.5 Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJCE, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.

7.1.6 Credenciar devidamente um Preposto para representá-lo em todas as questões relativas ao cumprimento dos serviços, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa com o TJCE e a equipe da CONTRATADA, sem custo adicional.

7.1.7 Assumir total responsabilidade pela execução dos serviços/entrega de bens contratados, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.

7.1.8 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.

7.1.9 Comunicar ao TJCE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços/entrega de bens, propondo as ações corretivas necessárias para a execução dos mesmos.

7.1.10 Submeter ao TJCE qualquer alteração que se tornar essencial à continuação da execução dos serviços/entrega de bens.

7.1.11 Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

7.1.12 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.

7.1.13 Selecionar e preparar rigorosamente o(s) empregado(s) que irá(ão) prestar os serviços;

7.1.14 Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência;

7.1.15 Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços/entrega de bens.

7.1.16 Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, realizando-os de forma meticulosa e constante, mantendo sempre em perfeita ordem;

7.1.17 Orientar seus empregados de que não poderão se retirar dos prédios ou instalações da Contratante portando volumes ou objetos sem a devida autorização e liberação do Fiscal do contrato.

7.1.18 Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do CONTRATANTE, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

7.1.19 Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento;

7.1.20 Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço/entrega de bens, ou em conexão com ele, ainda que acontecido em dependências do CONTRATANTE.

7.1.21 Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.

7.1.22 Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços/entrega de bens, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente;

7.1.23 Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.

7.1.24 Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua regularização.

7.1.25 Não transferir a outrem, no todo ou em parte, a execução do contrato;

7.1.26 Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir;

7.1.27 Responsabilizar-se pela conduta do empregado que for incompatível com as normas da Contratante, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação;

7.1.28 Receber as observações dos fiscais do contrato do contrato, relativamente ao desempenho das atividades/entrega de bens, e identificar as necessidades de melhoria;

7.1.29 Registrar e controlar, diariamente, as ocorrências e os serviços sob sua responsabilidade;

7.1.30 Permitir a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo Contratante, em conformidade com o artigo 117 da Lei nº 14.133/21;

7.1.31 Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21;

7.1.32 Indenizar quaisquer danos ou prejuízos causados ao TJCE ou a terceiros, por ação ou omissão do seu pessoal durante a execução dos serviços/entrega de bens;

7.1.33 Não colocar à disposição da Contratante, para o exercício de funções de chefia, pessoal que incidam na vedação dos artigos 1º e 2º da Resolução nº 156/2012 do Conselho Nacional de Justiça (Art. 4º - Resolução 156/2012 – CNJ).

7.1.34 Encaminhar para o atesto dos fiscais, as faturas emitidas dos serviços prestados/bens entregues.

7.1.35 Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o CONTRATANTE for compelido a responder em decorrência desta avença.

7.1.36 Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços/entrega de bens da relação contratual mantida com o CONTRATANTE.

7.1.37 Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

7.1.38 Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.

7.1.39 Comprovar vínculo empregatício dos profissionais disponibilizados para prestação dos serviços objeto desta contratação através de Ficha de Registro de Empregado, ou Carteira de Trabalho, ou contrato de prestação de serviço (ou documento similar) ou ainda Contrato Social da empresa, em casos de vínculo societário.

7.1.40 Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo contratante.

7.1.41 Não subcontratar, ceder ou transferir, total ou parcial o objeto desta contratação.

7.1.42 Recrutar e selecionar os profissionais necessários à realização do serviço, de acordo com a qualificação técnica exigida, a ser previamente submetida ao Fiscal para verificação da conformidade.

7.1.43 Fornecer ao TJCE ao início da prestação do serviço, relação nominal dos técnicos que atuarão no cumprimento do objeto contratado, atualizando-a sempre que necessário;

7.1.44 Tal documentação deverá ser juntada nos autos dos contratos.

7.1.45 Manter atualizada a documentação comprobatória da qualificação dos profissionais alocados na execução do serviço e disponibilizar essa documentação ao Tribunal, sempre que solicitada;

7.1.46 Manter o TJCE formalmente avisado sobre demissões de profissionais que prestem serviço nas dependências do Tribunal, para fins de cancelamento da autorização de entrada e acessos a recursos, sistemas e aplicativos do TJCE;

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

7.1.48 Conceder acesso ao TJCE do controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do mesmo.

8 Forma de Acompanhamento do Contrato

ID	Evento	Forma de Acompanhamento
1	Da entrega da solução	O recebimento do objeto deverá ocorrer conforme definido no item **5** e seus subitens.
2	Durante a vigência do Contrato.	Será verificado o cumprimento do prazo de solução dos cha-

		mados, conforme descrito neste termo.

8.1 Metodologia de Avaliação da Qualidade

8.1.1 Conforme item **5.12**.

8.2 Níveis de Serviço

8.2.1 Conforme itens **5.6 e 5.7**.

8.3 Estimativa do Volume de Bens/Serviço

ID	Bem	Estimativa	Forma de Estimativa
1	Firewall - Hardware	Duas Unidades	A quantidade de firewalls e todos os seus requisitos técnicos foram definidos após análise dos requisitos de negócio e técnicos da área demandante. Para a definição dos quantitativos, foram consideradas a atual quantidade de dois equipamentos utilizados na solução de segurança. O alinhamento entre os requisitos do objeto desta contratação e os requisitos da área de negócio estão detalhados nos estudos técnicos preliminares.
2	Software Gerenciamento centralizado e relatoria	Uma unidade	Para a definição dos quantitativos, foram consideradas a atual quantidade de equipamentos utilizados na solução de segurança.
3	Solução para acesso remoto seguro e a aplicações privadas	Licença para 2000 usuários	Para a definição dos quantitativos, foram consideradas a atual quantidade de usuários utilizando a solução atual de segurança.
4	Serviço de instalação	Uma unidade	Para a definição dos quantitativos, foram consideradas a quantidade de serviço necessário para instalação do novo equipamento a ser adquirido.

5	Serviço de suporte técnico e monitoramento 24x7	Serviço para 60 meses	Para a definição dos quantitativos, foram consideradas a quantidade de meses da garantia do novo equipamento a ser adquirido.
6	Treinamento	1 unidade para 8 pessoas	Para a definição dos quantitativos, foram consideradas a quantidade de servidores da SETIN com demandas da área de segurança da informação

8.4 Prazos e Condições

N.º	Etapa	Quando	Responsável
1	Reunião de alinhamento	Em até 5 (cinco) dias úteis após a data de assinatura do contrato.	CONTRATANTE e CONTRATADA
2	Entrega do hardware	Em até 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.	CONTRATADA
3	Instalação, configuração e testes da solução	Em até 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.	CONTRATADA
4	Conclusão da Instalação, configuração e testes da solução	Em até 15 (quinze) dias úteis contados a partir da data de emissão da ordem de serviço pela Contratada.	CONTRATADA
5	Operação assistida	Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na tabela do item 1.2, com duração de 20 dias úteis, podendo ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços até que sejam sanadas para o atendimento dos requisitos técnicos.	CONTRATADA
6	Treinamento	Está condicionada à solicitação prévia, via emissão de ordem de serviço por parte da Contratante, em data a ser previamente	CONTRATADA

		acordada com o TJCE.	
7	Documentação	Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço.	CONTRATADA
8	Início do período de validade/vigência dos licenciamentos. Início do período de prestação de serviço de suporte técnico e garantia da solução.	60 (sessenta) meses após a emissão do Termo de Recebimento Definitivo.	CONTRATADA
9	Regime para atendimento da garantia on-site	NBD - Next Business Day (próximo dia útil) em atendimento no regime 24x7 (24 horas por dia, 7 dias na semana).	CONTRATADA

8.5 Do Reajuste

8.5.1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de apresentação da proposta.

8.5.2 Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custo da Tecnologia da Informação (ICTI) - Ipea, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.5.2.1 O processo referente ao pedido de Reajuste supra deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.

8.6 Condições para Pagamento

8.6.1 Os pagamentos serão realizados através de depósito bancário preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade com as medições realizadas, validado previamente pela CONTRATANTE atestada pelo setor competente deste Tribunal de Justiça, via emissão do Termo de Recebimento Definitivo, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

8.6.2 O prazo para pagamento faturas ou notas fiscais serão suspensos durante o período de indisponibilidade do sistema de pagamento do Estado do Ceará ao final de cada exercício financeiro, aproximadamente entre 20 de dezembro e 31 de janeiro do ano subsequente, cujos pagamentos serão realizados até o final da primeira quinzena do mês de fevereiro.

8.6.3 O Tribunal de Justiça reserva-se ao direito de recusar o pagamento, no ato do atesto, caso o objeto não esteja em conformidade com as condições deste instrumento;

8.6.4 Nenhum pagamento será efetuado à empresa antes regularizada as sanções que por ventura lhe tenham sido aplicadas;

8.6.5 Nas notas fiscais referentes aos serviços objeto do contrato, deverão estar descriminados os valores dos tributos: impostos sobre serviços – ISS, PIS/PASEP, COFINS, FUST, FUNTTEL;

8.6.6 Os serviços de suporte e manutenção serão faturados mensalmente após a solicitação de pagamento por parte da CONTRATADA, sendo o pagamento condicionado ao aceite do Relatório de Instrumento de Medição de Resultados, item **5.5.4**, por parte da CONTRATANTE.

8.6.6.1 O valor do pagamento mensal estará diretamente vinculado ao índice alcançado para os indicadores estabelecidos, sendo pago conforme resultado obtido e decrementado (cumulativamente) quando não forem atingidas as metas exigidas.

8.6.6.2 Caso a CONTRATADA não cumpra com os seus compromissos, de qualidade e desempenho, terá a sua fatura reduzida conforme estabelecido no item **5.7.16**;

8.6.6.3 Os redutores deverão ser levantados pela Contratada, anexados à solicitação de pagamento, sendo validados pelo TJCE. Os redutores serão aplicados sobre o faturamento mensal na ocorrência dos fatos geradores, independentemente da abertura de processo administrativo.

8.6.7 Constatada a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

8.6.8 Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, 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.

8.6.9 Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

8.6.10 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação;

8.6.11 Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

8.6.12 Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) ser emitida(s) em nome do Tribunal de Justiça do Estado do Ceará, CNPJ N.º 09.444.530/0001-01 e em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

8.6.13 O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual;

8.6.14 Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

8.6.15 Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

8.6.16 A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

8.7 Propriedade, Sigilo, Restrições

8.7.1 A CONTRATADA cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do art. 30, da Lei Federal N.º 14.133/21, combinado com o art. 4.º, da Lei Federal N.º 9.609/98, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência do objeto contratado, entendendo-se por resultados quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros;

8.7.2 Toda a documentação produzida pela CONTRATADA referente à implantação dos equipamentos e documentos exigidos no termo de referência passam a ser propriedade de forma perpétua do TJCE, não precisando este Tribunal de autorização da CONTRATADA para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

8.7.3 Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso;

8.7.4 A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente;

8.7.5 Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados que, a qualquer título, venham a integrar a equipe executante do Objeto, a assinatura do **ANEXO II - TERMO DE CIÊNCIA**, bem como a assinatura do **ANEXO III - TERMO DE COMPROMISSO** onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

8.7.6 A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte, mediante assinatura do Termo de Confidencialidade constante no Termo de Referência.

8.8 Mecanismos Formais de Comunicação

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Emissão da Ordem de serviço/fornecimento	Contratante	Contratada	Ordem de serviço/fornecimento	Quando demandado pela SETIN.
Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
Abertura de chamados de garantia. Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado;	Contratante	Contratada	E-mail, telefone e site na internet	Quando demandado pela SETIN.
Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, email, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document*	Quando necessário

			Format): documento em formato portável.	

9 ESTIMATIVA DE PREÇO

Id	Bem/Serviço	Model/Part Number	Qtd.	Vlr. Unit Médio	Vlr. Total Médio
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2	R$ 652.367,61	R$ 1.304.735,22
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2	R$ 1.561.136,02	R$ 3.122.272,04
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2	R$ 482.258,32	R$ 964.516,64
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1	R$ 2.108.798,10	R$ 2.108.798,10
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1	R$ 67.731,11	R$ 67.731,11
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1	R$ 77.022,64	R$ 77.022,64
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2	R$ 562.446,50	R$ 1.124.893,00

8	Implantação da solução de Firewall	---	1	R$ 17.480,33	R$ 17.480,33
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	---	1	R$ 13.440,28	R$ 13.440,28
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	---	1	R$ 193.740,09	R$ 193.740,09
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	---	1	R$ 306.231,50	R$ 306.231,50
				Valor Total Global	**R$ 9.300.860,95**

10 ADEQUAÇÃO ORÇAMENTÁRIA

Objeto	Aquisição de novos *appliances* de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção pelo prazo de 60 (sessenta) meses; incluindo serviços de instalação, treinamento e demais especificações e características consignados neste Termo de Referência.
Fonte	Fundo Especial de Reaparelhamento e Modernização do Poder Judiciário do Estado do Ceará (FERMOJU)
Programa	192 - Excelência no desempenho da prestação jurisdicional
Ação	11470 – Desenvolvimento da Infraestrutura de TI – FERMOJU 11473 – Desenvolvimento da Infraestrutura de TI – FERMOJU 20511 – Apoio ao desenvolvimento da prestação - Jurisdicional na área de TI – FERMOJU (1° Grau) 20512 – Apoio ao desenvolvimento da prestação - Jurisdicional na área de TI – FERMOJU (2° Grau)
Natureza	Custeio/investimento

Fonte	Id	Bem/ Serviço	Qtd.	Vlr. Unit Médio	Vlr. Total Médio	Jurisdição do 1°	Jurisdição do 2°

FERMOJU	1	**BEM - PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks**	2	R$ 652.367,61	R$ 1.304.735,22	R$ 1.239.498,46	R$ 65.236,76
	2	**SERVIÇO - PA-5410 –60 meses– Palo**	2	R$ 1.561.136,02	R$ 3.122.272,04	R$ 2.107.533,63	R$ 1.014.738,41

	Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)					
3	**SERVIÇO - GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks**	2	R$ 482.258,32	R$ 964.516,64	R$ 651.048,73	R$ 313.467,91
4	**SERVIÇO - Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks**	1	R$ 2.108.798,10	R$ 2.108.798,10	R$ 1.423.438,72	R$ 685.359,38
5	**SERVIÇO - Panorama management software, 25 devices**	1	R$ 67.731,11	R$ 67.731,11	R$ 45.718,50	R$ 22.012,61

	60 meses – Palo Alto Networks					
6	**SERVIÇO - Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks**	1	R$ 77.022,64	R$ 77.022,64	R$ 51.990,28	R$ 25.032,36
7	**SERVIÇO - Premium support term, PA-5410 60 meses – Palo Alto Networks**	2	R$ 562.446,50	R$ 1.124.893,00	R$ 759.302,78	R$ 365.590,23
8	**SERVIÇO - Implantação da solução de Firewall**	1	R$ 17.480,33	R$ 17.480,33	R$ 11.799,22	R$ 5.681,11
9	**SERVIÇO - Treinamento para até 08 (oito) pessoas. Carga horária de 40h**	1	R$ 13.440,28	R$ 13.440,28	R$ 9.072,19	R$ 4.368,09
10	**SERVIÇO - Serviço de instalação e repasse de conhecimento para solução de zero trust**	1	R$ 193.740,09	R$ 193.740,09	R$ 130.774,56	R$ 62.965,53

		network access (ztna)					
	11	**SERVIÇO - Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses**	1	R$ 306.231,50	R$ 306.231,50	R$ 206.706,26	R$ 99.525,24
						R$ 6.636.883,33	**R$ 2.663.977,62**
					Valor Total Global	**R$ 9.300.860,95**	

11 SANÇÕES APLICÁVEIS

11.1 Comete infração administrativa, nos termos da lei, a licitante que:

11.1.1 Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pela Administração, em sede de diligência;

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

11.1.2.1 não enviar a proposta ajustada após a negociação;

11.1.2.2 recusar-se a enviar o detalhamento da proposta quando exigível;

11.1.2.3 pedir para ser desclassificado quando encerrada a etapa competitiva;

11.1.2.4 deixar de apresentar amostra, quando exigível;

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

11.1.4 Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

11.1.5 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

11.1.6 Fraudar a licitação;

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

11.1.7.1 agir em conluio ou em desconformidade com a lei;

11.1.7.2 induzir deliberadamente a erro no julgamento;

11.1.7.3 apresentar amostra falsificada ou deteriorada;

11.1.7.4 praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

11.1.7.5 praticar ato lesivo previsto no art. 5° da Lei 12.846/2013;

11.2 A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido no instrumento convocatório, descrita no item **11.1**, inciso IV, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

11.2.1 A exigência da garantia de que trata o subitem anterior, obedecerá ao disposto no art. 58 da Lei nº 14.133/2021.

11.3 Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar a contratada as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

11.3.1 Advertência;

11.3.2 Multa;

11.3.3 impedimento de licitar e contratar; e

11.3.4 Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade;

11.4 Na aplicação das sanções serão considerados:

11.4.1 a natureza e a gravidade da infração cometida;

11.4.2 as peculiaridades do caso concreto;

11.4.3 as circunstâncias agravantes ou atenuantes;

11.4.4 os danos que dela provierem para a Administração Pública;

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

11.5 A sanção de multa calculada na forma do edital ou do contrato, não será inferior a 0,5% (cinco décimos por cento), nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.

11.5.1 A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o

complementem, às sanções e penalidades administrativas, inclusive multas.

11.5.1.1 Caso a Contratada se torne inadimplente na execução dos serviços, a Contratante poderá, sem prejuízo de outras medidas, a título de multa, o equivalente a 0,5% (cinco décimos por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, para a conclusão da demanda, nos termos e condições dispostas no Termo de Referência, sem prejuízo das sanções legais e responsabilidades civil e criminal.

11.5.2 A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

11.5.3 Os percentuais de multas aplicadas incidirão sempre sobre do valor global do termo de contrato licitado ou celebrado ou instrumento equivalente.

11.6 As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

11.7 Na aplicação da sanção será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

11.8 A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no item 11.1, incisos I, II e III, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

11.9 Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas no item 11.1, incisos IV, V, VI e VII, bem como pelas infrações administrativas previstas no item 11.1, incisos I, II e III que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

11.10 A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.11 Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual 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, que deverá proferir

sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

11.12 Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

11.13 O recurso e o pedido de reconsideração terão ef eito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14 A aplicação das sanções previstas neste termo de referência não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

11.15 Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

11.16 As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.

11.17 Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando - se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

11.18 Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 156 da Lei n. 14.133/21:

11.18.1 Aplicação de multa administrativa, além daquelas previstas no item **5.7**.

11.18.1.1 Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo.

11.18.1.2 Na ordem de 0,5% do valor total da contratação, ao dia de suspenção ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços de instalação, configuração, suporte técnico ao total de 10%, moratório.

11.18.1.3 Na ordem de 1% sobre o valor da Nota Fiscal em questão, ao dia pelo não cumprimento do conteúdo disposto nos itens **5.3.6** e **5.11.5.11** deste Termo de Referência, limitado ao total de 20%.

11.18.1.4 Caso os limites dos subitens **11.18.1.2 e 11.18.1.3** sejam excedidos, configura-se então casos de inexecução contratual.

12 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1 Proposta de Preço

12.1.1 A proposta deverá conter obrigatoriamente os seguintes elementos:

12.1.1.1 Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

12.1.1.2 Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

12.1.1.3 Deve fazer menção ao número do pregão e do processo licitatório;

12.1.1.4 Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

12.1.1.5 Deve conter na última folha o número do CNPJ da empresa;

12.1.1.6 Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

12.1.1.7 Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a licitante julgar necessário;

12.1.1.8 Indicação do nome do banco, número da agência, número da conta corrente, para fins de recebimento dos pagamentos.

12.1.2 Tipo de Licitação

12.1.2.1 A licitação será do tipo menor preço. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item **9**.

12.1.2.2 O objeto desta contratação será realizado por execução indireta, sob o regime de empreitada por Preço Unitário, nos termos dos art. 46°, I, da Lei n. 14.133/21.

12.2 Justificativa de Adoção da Modalidade da Licitação

12.2.1 Modalidade de Licitação

12.2.2 A contratação da solução ora pretendida é oferecida por diversos fornecedores no mercado de TIC, vez que apresenta características padronizadas e usuais. Assim, trata-se de serviços e bens comuns, uma vez que é fácil encontrar empresas no mercado que ofereçam serviços de manutenção, suporte e garantia da Solução pretendida. Devido à alta demanda por esses serviços, há uma ampla oferta de fornecedores com diferentes níveis de expertise e qualidade e, portanto, licitação via Pregão, em sua forma eletrônica, pelo tipo menor preço, previamente ao menor preço de cada item, e modo de disputa aberto e fechado.

12.3 Qualificação Econômico-Financeira

12.3.1 A Qualificação Econômico-Financeira tem como objetivo avaliar a capacidade financeira e econômica das empresas interessadas em participar da concorrência, garantindo assim a segurança do contrato e a viabilidade do projeto. No Tribunal de Justiça do Ceará, a Qualificação Econômico-Financeira é um critério importante para a escolha da empresa vencedora, pois garante a solvência financeira e a capacidade de cumprimento do contrato firmado.

12.3.2 Certidão negativa de falência, concordata, recuperação judicial ou extrajudicial, expedida por quem de competência na sede da pessoa jurídica ou certidão negativa de execução patrimonial expedida no domicílio da pessoa física.

12.3.3 No caso de cooperativa, a mesma está dispensada da apresentação da Certidão exigida no subitem acima.

12.3.4 **BALANÇO PATRIMONIAL** e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira do licitante, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 meses da data de apresentação da proposta.

12.3.5 **COMPROVAÇÃO DA BOA SITUAÇÃO FINANCEIRA** atestada por documento, assinado por profissional legalmente habilitado junto ao Conselho Regional de Contabilidade da sede ou filial do licitante, demonstrando que a empresa apresenta

índice de Liquidez Geral (LG) maior ou igual a 1,0 (um vírgula zero), calculada conforme a fórmula abaixo:

$$LG = (AC + ARLP)/(PC + PELP) \geq 1,0$$

Onde:
LG – Liquidez Geral;
AC – Ativo Circulante;
ARLP – Ativo Realizável a Longo Prazo;
PC – Passivo Circulante;
PELP – Passivo Exigível a Longo Prazo;

12.3.6 No caso de sociedade por ações, o balanço deverá ser acompanhado da publicação em jornal oficial, em jornal de grande circulação e do registro na Junta Comercial.

12.3.7 No caso das demais sociedades empresárias, o balanço deverá ser acompanhado dos termos de abertura e de encerramento do Livro Diário - estes termos devidamente registrados na Junta Comercial - constando ainda, no balanço, o número do Livro Diário e das folhas nos quais se acha transcrito ou autenticada na junta comercial, devendo tanto o balanço quanto os termos ser assinados por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

12.3.8 No caso de empresa recém-constituída (há menos de 01 ano), deverá ser apresentado o balanço de abertura acompanhado dos termos de abertura e de encerramento devidamente registrados na Junta Comercial, constando no balanço o número do Livro e das folhas nos quais se acha transcrito ou autenticado na junta comercial, devendo ser assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

12.3.9 No caso de sociedade simples e cooperativa - o balanço patrimonial deverá ser inscrito no Cartório de Registro Civil de Pessoas Jurídicas assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da instituição, atendendo aos índices estabelecidos neste instrumento convocatório.

12.3.10 **PATRIMÔNIO LÍQUIDO MÍNIMO** não inferior a 10% da estimativa de custos, que deverá ser comprovado através da apresentação do balanço patrimonial.

12.3.11 A comprovação solicitada visa garantir que a CONTRATADA possua capacidade e porte suficiente para atender ao objeto desta contratação, bem como a capacidade financeira de sustentar suas atividades diante das oscilações de demandas que ocorrem durante a vigência do contrato.

12.4 Qualificação Técnica

12.4.1 Com o intuito de minimizar os riscos da contratação e alcançar os resultados esperados, é imprescindível que o LICITANTE possua capacidade técnica e de fornecimento para executar o objeto da licitação;

12.4.2 A exigência de comprovação de capacidade técnica relacionada ao objeto licitado se dá com fulcro no art. 67 inciso I da Lei nº 14.133/21 e visa garantir que a LICITANTE já forneceu os serviços a serem contratados e, portanto, possui capacidade técnico-operacional para fornecê-lo adequadamente;

12.4.3 A Licitante classificada deverá apresentar, para fins de habilitação, 1 (um) ou mais atestados de capacidade técnica, exclusivamente em seu nome, expedidos por pessoa jurídica de direito público ou privado, que comprovem:

12.4.3.1 A **entrega, instalação e configuração** de 50% da quantidade dos equipamentos similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação do mesmo fabricante;

12.4.3.2 A execução do serviço de suporte técnico com garantia de solução de Firewall, pelo menos, 12 (doze) meses ininterruptos;

12.4.4 Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária da CONTRATADA, especificadas no contrato social vigente;

12.4.5 Os quantitativos acima mencionados foram definidos com base na demanda a ser contratada, de modo a não exceder 50% dele.

12.4.6 Tendo em vista que os atestados de capacidade de entrega de equipamentos se limitam a 1 (uma) unidade de cada item, não será aceito somatório de atestados.

12.4.7 A LICITANTE disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados.

12.4.8 No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da LICITANTE. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente;

12.4.9 O TJCE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas no Termo de Referência, podendo buscar por meios próprios ou exigir a apresentação de documentação complementar, tais como Notas Fiscais, Contratos, Atas do Pregão Original, entre outros, referente à prestação de serviços relativos aos atestados apresentados;

12.4.10 A comprovação de capacidade técnica estará sujeita à confirmação da veracidade de suas informações através de possíveis diligências, conforme prescreve o art. 59, § 2º, da Lei 14.133/21.

12.4.11 Caso a LICITANTE não comprove as exigências previstas neste Termo de Referência por meio das documentações requeridas, será desclassificada.

12.4.12 O atestado deverá conter:

12.4.12.1 Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

12.4.12.2 Razão Social da Contratada;

12.4.12.3 Número e vigência do contrato;

12.4.12.4 Objeto do contrato;

12.4.12.5 Descrição do trabalho realizado;

12.4.12.6 Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento de cronogramas pactuados;

12.4.12.7 Local e Data de Emissão;

12.4.12.8 Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);

12.4.12.9 Assinatura do responsável pela emissão do atestado;

12.4.13 Deve possuir, ainda, registro comercial, em caso de empresa individual.

12.4.14 A não comprovação de alguma característica exigida, quando solicitada pelo Contratante, levará à desclassificação da proposta.

12.4.15 Tratando-se de empresa ou sociedade estrangeira em funcionamento no país, deve possuir Decreto de Autorização e Ato de Registro, ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

12.4.16 Ressalta-se que a licitante deve atuar no ramo pertinente ao objeto da licitação, tendo como atividade aquela compatível com os materiais descritos neste Termo de Referência.

12.4.17 Por fim, caso a empresa esteja sob falência, concurso de credores, dissolução ou liquidação, deve apresentar Plano de Recuperação Judicial, devidamente homologado. Se nessas condições e, ainda, sendo formada em consórcio de empresas, esta não deverá ser controladora, coligada ou subsidiária entre si, devendo, da mesma forma, apresentar Plano de Recuperação Judicial, devidamente homologado.

13 GARANTIA CONTRATUAL

13.1 A CONTRATADA deverá entregar ao Gerente de Contratação do objeto, que submeterá à Coordenadoria Central de Contratos e Convênios do TJCE, no prazo prescrito no art. 96 da Lei n.º 14.133/2021, a título de garantia, a quantia equivalente a 5% (cinco por cento) do valor global da contratação, cabendo-lhe optar dentre as modalidades previstas no art. 96, Lei n.º 14.133/2021.

13.1.1 A garantia será devolvida à CONTRATADA somente depois do cumprimento integral das obrigações assumidas, inclusive recolhimento de multas e satisfação de prejuízos causados ao CONTRATANTE.

13.1.2 Será exigida do licitante vencedor a indicação na sua proposta a modalidade da garantia escolhida, a fim de possibilitar a contagem do prazo de acordo com cada modalidade.

13.2 A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

13.2.1 Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

13.2.2 Prejuízos causados à administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

13.2.3 As multas moratórias e punitivas aplicadas pelo CONTRATANTE à CONTRATADA;

13.2.4 Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

13.3 A contratada terá o prazo mínimo de 1 (um) mês, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pela modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

13.3.1 A apólice deverá seguir as regras estatuídas na Circular Susep nº 662, de 11 de abril de 2022, quando da escolha por parte do licitante vencedor da modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

13.3.2 O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas, conforme inciso II do artigo 97 da Lei Nº 14.133/21.

13.3.3 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados neste documento, observada a legislação que rege a matéria.

13.4 A contratada terá o prazo mínimo de 10 (dez) dias corridos, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pelas demais modalidades previstas no § 1º do art. 96, da Lei Nº 14.133/21.

13.4.1 A garantia em dinheiro deverá ser efetuada em instituição bancária indicada pelo CONTRATANTE, com correção monetária, em favor do CONTRATANTE.

13.4.2 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

13.4.3 No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

13.5 A garantia deverá ter validade durante a execução do contrato de 90 (noventa) dias após término da vigência contratual, devendo acompanhar as modificações referentes ao valor e à vigência desta mediante a complementação da caução ou emissão do respectivo endosso pela seguradora ou instituição bancária fiadora.

13.5.1 O prazo para complementação da caução ou emissão do endosso da garantia referente aos aditivos contratuais deverá seguir os mesmos prazos estabelecidos nos subitens **13.3 e 13.4**.

13.6 Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento de multas, ela deve ser complementada no prazo de até 10 (dez) dias úteis, contados da solicitação do

CONTRATANTE, a partir do qual se observará o disposto abaixo:

13.6.1 A não complementação ou renovação, tempestiva, da garantia do contrato ensejará a suspensão de pagamentos até a regularização do respectivo documento, independentemente da aplicação das sanções contratuais.

13.6.2 A inobservância do prazo fixado para apresentação, complementação ou renovação da garantia acarretará a aplicação das sanções previstas neste Termo de Referência.

13.7 O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

13.8 A garantia será considerada extinta:

13.8.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro ou títulos da dívida pública, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;

13.8.2 No prazo de 90 (noventa) após o término da vigência, caso o CONTRATANTE não comunique a ocorrência de sinistros.

13.9 A ausência de prestação da garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa e rescisão unilateral do contrato administrativo.

14 DA ASSINATURA DO CONTRATO

14.1 A licitante vencedora deverá assinar o Contrato dentro do prazo de 5(cinco) dias úteis, contados a partir da sua convocação.

14.2 O prazo estabelecido no subitem anterior poderá ser prorrogado uma vez, por igual período, quando solicitado pelo fornecedor e desde que ocorra motivo justificado aceito pela Administração.

14.3 A recusa injustificada do licitante vencedor em assinar o contrato, dentro do prazo estabelecido no subitem **14.1**, ensejará a aplicação das penalidades previstas no instrumento convocatório.

15 VIGÊNCIA CONTRATUAL

15.1 A vigência do contrato inicia na data de sua assinatura vigorará por até 60 (sessenta) meses, podendo ser prorrogado sucessivamente, respeitando a vigência máxima de dez anos, conforme previsto na legislação.

15.2 A escolha do prazo de 60 (sessenta) meses de vigência baseia-se não somente no investimento, mas também na continuidade e no desempenho de funções de segurança da informação do TJCE, agregado à possibilidade de renovação, até o limite permitido pela atual legislação, desde que se comprove vantajoso ao TJCE.

15.3 O prazo dilatado permitirá obtenção de ganho de escala, reduzindo o grau de incerteza da contratação e consequentemente melhores preços para a Administração;

15.4 Ademais, é maior a atratividade do certame pelo mercado, por meio de uma maior diluição dos custos por durante o lapso temporal do contrato, favorecendo a Administração em termos de economicidade e ampliação da competitividade;

15.5 Como também está alinhada ao padrão praticado no mercado, como pode ser verificado nas contratações públicas similares.

15.6 Por se tratar de um objeto de execução crítica e de tamanha importância para o judiciário cearense, como também foi definida acima, a importância da solução a ser adquirida, vemos também, a importância e quão crítica é a perfeita execução do objeto e a relevância de uma manutenção e suporte contínuo. Garantindo qualidade e eficiência no funcionamento da Solução, bem como a facilidade e eficiência na gestão do contrato para a Administração.

15.7 A contratação em tela envolve serviços críticos, necessários à conservação do futuro patrimônio público, objeto desta contratação acima descrito, e ao bom andamento das atividades judiciárias e administrativas desenvolvidas pelo Poder Judiciário Cearense e, consequentemente, para toda a sociedade de modo geral.

15.8 Atenta-se, nesse sentido, ao entendimento da Corte de Contas da União, quando em seu Acórdão n° 132/2008, da Segunda Câmara, sob relatoria do Ministro Aroldo Cedraz, prescreve que contratos dessa natureza intentam "manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional".

15.9 Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, suporte e garantia inerentes a solução a ser adquirida, sobretudo os utilizados pelo TJCE, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos.

15.10 Devido à importância destes serviços e no intuito de sempre melhor atender às demandas de manutenção, de suporte e de garantia, inerentes à solução a ser adquirida, além dos significativos acréscimos de serviços em relação ao escopo de trabalho atual, em função das demandas de crescimento e ampliação dos serviços judiciais e administrativos, e a imperiosidade da sua prestação ininterrupta em face do desenvolvimento habitual das atividades administrativas, sob pena de prejuízo ao interesse público, denota-se necessária a contratação pelo tempo indicado, conforme descrito neste documento.

15.11 Diante do exposto, considera-se de extrema relevância para a Administração a contratação do objeto em tela, entendendo imprescindível a vigência do termo de contrato por até 60 (sessenta) meses, contados da data de emissão do Termo de Recebimento Definitivo.

Equipe de Planejamento da Contratação

Heldir Sampaio Silva – 9630	Fábio de Carvalho Leite – 9594	Cristiano Henrique Lima de Carvalho – 5198
Integrante Técnico	Integrante Administrativo	Área Demandante e Integrante Demandante

16 APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Licitação para iniciação de procedimento licitatório, segundo o art. 53 da Lei nº 14.133/2021.

Autoridade Competente

Denise Maria Norões Olsen – 24667

Área de Tecnologia da Informação

Fortaleza, 06 de maio de 2024

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

Id	Bem/Serviço	Model/Part Num-ber	Qtd.
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2
8	Implantação da solução de Firewall	---	1
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	---	1
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	---	1
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	---	1

2. ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

2.1. NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.1.1. CARACTERÍSTICAS GERAIS

2.1.1.1. A solução deve incluir um par de equipamentos (appliances) Next Generation Firewall em alta disponibilidade, bem como uma solução

de gerenciamento centralizado e relatoria, todos fornecidos pelo mesmo fabricante. Cada par de equipamentos de alta disponibilidade deve ser projetado especificamente para a função de Next Generation Firewall, com hardware e software também provenientes do mesmo fabricante.

2.1.1.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, de forma integrada e simultânea, as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware Protection, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL;

2.1.1.3. O equipamento e seus componentes deverão ser novos, sem uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

2.1.1.4. Não será aceito equipamento em modo End of Life e End of Support.

2.1.1.5. Não serão aceitas soluções baseadas em PCs de uso geral.

2.1.1.6. A solução deve suportar a configuraçao de alta disponibilidade, podendo ser configurado ativo/passivo ou ativo/ativo, com consideração para licenciamento adicional, se necessário.

2.1.1.7. Todos os componentes necessários para o pleno funcionamento da solução devem ser fornecidos.

2.1.1.8. Todas as funcionalidades que dependam de licenciamento devem ser entregues licenciadas para 60 meses.

2.1.2. CARACTERÍSTICAS FÍSICAS MÍNIMAS

2.1.2.1. Deve possuir throughput de, no mínimo, 26 Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

2.1.2.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, e estar licenciado para a criação de pelo menos 10 (dez) sistemas virtuais, independentes entre si.

2.1.2.3. Deve suportar, no mínimo, 3.500.000 conexões simultâneas;

2.1.2.4. Deve suportar, no mínimo, 250.000 novas conexões por segundo;

2.1.2.5. Deve suportar, no mínimo, 7 (sete) Gbps de throughput de Inspeção SSL;

2.1.2.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo RJ-45;

2.1.2.7. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+.

2.1.2.8. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 40/100 Gbps do tipo QSFP+/QSFP28.

2.1.2.9. Deve possuir, no mínimo, 2 (duas) interface física dedicada para

o sincronismo de estados da solução de alta disponibilidade;

2.1.2.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

2.1.2.11. Deve possuir, no mínimo, 1 (uma) interface dedicada para gerenciamento;

2.1.2.12. Deve possuir armazenamento interno redundante de, no mínimo, 480 GB;

2.1.2.13. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 e 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento; deverá vir acompanhado de cabo de alimentação.

2.1.2.14. O equipamento deve ser fornecido com as portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para uso, sem custos adicionais. Todas as interfaces solicitadas nos appliances devem estar licenciadas e prontas para uso imediato, incluindo os transceivers/transceptores considerando o padrão Short Range (SR).

2.1.3. FUNCIONALIDADE DE FIREWALL

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

2.1.3.2. Suporte aos protocolos IPv4 e IPv6.

2.1.3.3. Suporte a no mínimo 512 VLANs no padrão 802.1q

2.1.3.4. Agregação de links 802.3ad e LACP;

2.1.3.5. Policy based routing ou policy-based forwarding;

2.1.3.6. Roteamento multicast (PIM-SM);

2.1.3.7. Deve suportar os protocolos IGMP v2, IGMP v3;

2.1.3.8. Deve suportar os protocolos DHCP e DHCPv6;

2.1.3.9. Deve suportar o protocolo NTP;

2.1.3.10. Jumbo Frames;

2.1.3.11. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

2.1.3.12. Suportar sub-interfaces ethernet logicas;

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

2.1.3.14. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;

2.1.3.15. Enviar log para sistemas de monitoração externos;

2.1.3.16. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

2.1.3.17. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

2.1.3.18. Proteção contra anti-spoofing;

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

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

2.1.3.21. Suportar a OSPF graceful restart;

2.1.3.22. Deve suportar o protocolo MP-BGP (Multiprotocol BGP)

permitindo que o firewall possa anunciar rotas para IPv4 e IPv6;

2.1.3.23. 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);

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

2.1.3.25. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

2.1.3.26. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

2.1.3.27. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

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

2.1.3.29. A configuração em alta disponibilidade deve sincronizar:

2.1.3.29.1. Sessões;

2.1.3.29.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

2.1.3.29.3. Certificados de-criptografados;

2.1.3.29.4. Associações de Segurança das VPNs;

2.1.3.29.5. Tabelas FIB;

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

2.1.4. CONTROLE POR POLÍTICA DE FIREWALL

2.1.4.1. Deverá suportar controles por zona de segurança;

2.1.4.2. Controles de políticas por porta e protocolo;

2.1.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

2.1.4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.1.4.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

2.1.4.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

2.1.4.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

2.1.4.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

2.1.4.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

2.1.4.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

2.1.4.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e 1.3;

2.1.4.12. Controle de inspeção e de-criptografia de SSH por política;

2.1.4.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

2.1.4.14. Bloqueios de arquivos por extensão;

2.1.4.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

2.1.4.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

2.1.4.17. Suporte a objetos e regras IPV6;

2.1.4.18. Suporte a objetos e regras multicast;

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

2.1.5. CONTROLE DE APLICAÇÕES

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

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

2.1.5.3. Reconhecer pelo menos 3000 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;

2.1.5.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

2.1.5.5. 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;

2.1.5.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

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

2.1.5.8. Atualizar a base de assinaturas de aplicações automaticamente;

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

2.1.5.10. 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;

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

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

2.1.5.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

2.1.5.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações customizadas;

2.1.5.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

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

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

2.1.5.18. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

2.1.5.19. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

2.1.5.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

2.1.5.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

2.1.6. IDENTIFICAÇÃO DE USUÁRIOS

2.1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

2.1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.1.6.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.1.6.4. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

2.1.6.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via syslog, para a identificação de endereços IP e usuários;

2.1.6.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

2.1.6.7. Suporte a autenticação Kerberos;

2.1.6.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

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

2.1.6.10. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;

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

2.1.7. QOS

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

2.1.7.2. Suportar a criação de políticas de QoS por:

2.1.7.3. Endereço de origem

2.1.7.4. Endereço de destino

2.1.7.5. Por usuário e grupo do LDAP/AD.

2.1.7.6. Por aplicações;

2.1.7.7. Por porta;

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

2.1.7.9. Banda Garantida

2.1.7.10. Banda Máxima

2.1.7.11. Fila de Prioridade.

2.1.7.12. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

2.1.7.13. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

2.1.7.14. Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

2.1.7.15. Deve suportar QOS (traffic-shapping), em interface agregadas;

2.1.7.16. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

2.1.8. VPN

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

2.1.8.2. Suportar IPSec VPN;

2.1.8.3. Suportar SSL VPN;

2.1.8.4. A VPN IPSEc deve suportar:

2.1.8.5. 3DES;

2.1.8.6. Autenticação MD5 e SHA-1;

2.1.8.7. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

2.1.8.8. Algoritmo Internet Key Exchange (IKEv1 e v2);

2.1.8.9. AES 128 e 256 (Advanced Encryption Standard);

2.1.8.10. Autenticação via certificado IKE PKI;

2.1.8.11. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

2.1.8.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

2.1.8.13. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

2.1.8.14. Deve suportar a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

2.1.8.15. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

2.1.8.16. O cliente de VPN SSL deve ser capaz de ser insalado e estar devidamente licenciado para criar perfis customizados de conformidade no mínimo os seguintes sistemas operacionais:

- **2.1.8.16.1.** Windows;
- **2.1.8.16.2.** MacOS
- **2.1.8.16.3.** Linux;
- **2.1.8.16.4.** Android
- **2.1.8.16.5.** Apple iOS.

2.1.8.17. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

2.1.8.18. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto:

- **2.1.8.18.1.** Sistema operacional e patches instalados;
- **2.1.8.18.2.** Antivírus e versão instalada;
- **2.1.8.18.3.** Firewall no host;
- **2.1.8.18.4.** Criptografia do disco;
- **2.1.8.18.5.** Agente de DLP instalado;
- **2.1.8.18.6.** Backup de disco;
- **2.1.8.18.7.** Chaves de registros;
- **2.1.8.18.8.** Processos ativos.

2.1.8.19. Deve permitir a quarentena automática e manual de dispositivos caso encontre algum comprometimento malicioso no tráfego inspecionado.

2.1.8.20. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções:

- **2.1.8.20.1.** sistema operacional e patches instalados;
- **2.1.8.20.2.** Antivírus e versão instalada;
- **2.1.8.20.3.** Firewall no host;
- **2.1.8.20.4.** Criptografia do disco;
- **2.1.8.20.5.** Agente de DLP instalado backup de disco;
- **2.1.8.20.6.** Chaves de registros
- **2.1.8.20.7.** Processos ativos;

2.1.9. PREVENÇÃO DE AMEAÇAS

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

2.1.9.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

2.1.9.3. 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;

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

2.1.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

2.1.9.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

2.1.9.7. Deve permitir o bloqueio de vulnerabilidades.

2.1.9.8. Deve permitir o bloqueio de exploits conhecidos.

2.1.9.9. Deve incluir proteção contra ataques de negação de serviços.

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

2.1.9.11. Análise de padrões de estado de conexões;

2.1.9.12. Análise de decodificação de protocolo;

2.1.9.13. Análise para detecção de anomalias de protocolo;

2.1.9.14. Análise heurística;

2.1.9.15. IP Defragmentation;

2.1.9.16. Remontagem de pacotes de TCP;

2.1.9.17. Bloqueio de pacotes malformados.

2.1.9.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

2.1.9.19. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

2.1.9.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

2.1.9.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.1.9.22. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

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

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

2.1.9.25. Identificar e bloquear comunicação com botnets;

2.1.9.26. Deve ser capaz de analisar em tempo real através de mecanismos baseados em Machine Learning o tráfego de ameaças avançadas de C2 (comando e controle) e spyware para proteção de ameaças de dia zero.

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

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

2.1.9.27.2. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;

2.1.9.27.3. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

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

2.1.9.27.5. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

2.1.9.27.6. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;

2.1.9.27.7. Rastreamento de vírus em pdf;

2.1.9.27.8. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

2.1.10. FILTRO WEB

2.1.10.1. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

2.1.10.2. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

2.1.10.3. Deve possuir pelo menos 60 categorias de URLs;

2.1.10.4. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.1.10.5. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

2.1.10.6. Deve suportar a capacidade de criação de políticas baseadas no controle por URL ou categoria de URL;

2.1.10.7. Deve suportar a criação categorias de URLs customizadas;

2.1.10.8. Deve possuir a função de exclusão de URLs do bloqueio;

2.1.10.9. Deve permitir a customização de página de bloqueio;

2.1.10.10. Deve 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);

2.1.10.11. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;

2.1.10.12. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

2.1.10.13. Deve prover análise em tempo real do conteúdo web e dessa forma permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução;

2.1.10.14. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

2.1.11. ANÁLISE DE MALWARES MODERNOS

2.1.11.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

2.1.11.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

2.1.11.3. Suportar a análise de arquivos maliciosos em ambiente

controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Android, Linux.

2.1.11.4. A solução deve possuir a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

2.1.11.5. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

2.1.11.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

2.1.11.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

2.1.11.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

2.1.11.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

2.1.11.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

2.1.11.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

2.1.11.12. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.1.11.13. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

2.1.11.14. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

2.1.11.15. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

2.1.11.16. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função.

2.1.11.17. Deve previnir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

2.1.11.18. Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable), ELF (executable and linked format) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos;

2.1.12. PROTEÇÃO DNS

2.1.12.1. Deve possuir a função resolução de endereços via DNS, para que

conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

2.1.12.2. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.1.12.2.1. Domínio suspeito identificado;

2.1.12.2.2. ID de assinatura de detecção;

2.1.12.2.3. Usuário logado na estação/servidor que originou o tráfego;

2.1.12.2.4. Aplicação;

2.1.12.2.5. Porta de destino;

2.1.12.2.6. IP de origem;

2.1.12.2.7. IP de destino;

2.1.12.2.8. Horário;

2.1.12.2.9. Ação do firewall;

2.1.12.2.10. Severidade;

2.1.12.2.11. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.1.12.2.12. A análise automática deve incluir, no mínimo, as seguintes características:

2.1.12.2.13. Padrões de consulta;

2.1.12.2.14. Entropia;

2.1.12.2.15. Análise de frequência n-gram de domínios;

2.1.12.2.16. Taxa de consultas.

2.1.12.2.17. Deve possuir a capacidade de analisar em tempo real a requisições de DNS e acesso a novas assinaturas de DNS;

2.1.13.SDWAN

2.1.13.1. Deve ser capaz de agregar vários links em uma interface virtual;

2.1.13.2. Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jiter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras da interface virtual;

2.1.13.3. Deve poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNS);

2.1.13.4. Deve suportar a agregação de túneis de VPN IPSec e balancear o tráfego entre eles e inserir essa interface agregada à Interface Virtual;

2.1.13.5. Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface virtual;

2.1.13.6. Deve possibilitar a distribuição de trafego entre os links que compõe a interface virtual, a critério do administrador;

2.1.13.7. Deve suportar a critério do administrador uma topologia Full-mesh;

2.1.13.8. Deve permitir configurar acesso direto à Internet para aplicações tipo SaaS;

2.1.13.9. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponiveis que

está orientado ao mesmo destino.

2.1.13.10. O dispositivo de SD-WAN deve utilizar Forward Error Correction (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

2.1.14. SUPORTE E GARANTIA DO FABRICANTE

2.1.14.1. Deve operar no regime 24/7;

2.1.14.2. Deve ser possivel abrir chamados telefonicos diretamente no fabricante no modelo 24/7;

2.1.14.3. Deve ter um tempo de resposta para chamados críticos de até 1 (uma hora);

2.1.14.4. Em caso de falha de hardware o envio do equipamento para a substituição deve operar no modo NBD (Next Business Day);

2.2. SOFTWARE PARA GERENCIAMENTO CENTRALIZADO DO CLUSTER DE FIREWALLS

2.2.1. O appliance virtual deve ser compatível com VMware ESXi, Microsoft Hyper-V e KVM;

2.2.2. Deve possuir capacidade de armazenamento de até 24TB;

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

2.2.4. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

2.2.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

2.2.6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

2.2.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

2.2.8. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;

2.2.9. Deve permitir a criação de objetos e políticas compartilhadas;

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

2.2.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;

2.2.12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

2.2.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

2.2.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

2.2.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou

WEB (HTTPS) e API aberta;

2.2.16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

2.2.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

2.2.18. O gerenciamento deve permitir/possuir:

- **2.2.18.1.** Criação e administração de políticas de firewall e controle de aplicação;
- **2.2.18.2.** Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- **2.2.18.3.** Criação e administração de políticas de Filtro de URL;
- **2.2.18.4.** Monitoração de logs;
- **2.2.18.5.** Ferramentas de investigação de logs;
- **2.2.18.6.** Debugging;
- **2.2.18.7.** Captura de pacotes.
- **2.2.18.8.** Acesso concorrente de administradores;

2.2.19. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

2.2.20. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

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

2.2.22. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

2.2.23. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

2.2.24. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

2.2.25. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

2.2.26. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.2.27. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

2.2.28. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

2.2.29. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

2.2.30. Criação de regras que fiquem ativas em horário definido;
2.2.31. Criação de regras com data de expiração;
2.2.32. Backup das configurações e rollback de configuração para a última configuração salva;
2.2.33. Suportar Rollback de Sistema Operacional para a ultima versão local;
2.2.34. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
2.2.35. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
2.2.36. Deve suportar interface de configuração baseada no padrão Openconfig.
2.2.37. Validação de regras antes da aplicação;
2.2.38. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
2.2.39. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
2.2.40. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
2.2.41. Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada.
2.2.42. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
2.2.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
2.2.44. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;
2.2.45. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
2.2.46. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
2.2.47. Deve ter a capacidade de encaminhar todo tráfego seja ele criptografado ou não para uma cadeia de equipamentos de segurança tais como IPS, IDS e SIEM para inspeção. Esta funcionalidade pode ser entregue por ferramenta externa.
2.2.48. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
2.2.49. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
2.2.50. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
2.2.51. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças

identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

2.2.52. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

2.2.53. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

2.2.54. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

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

2.2.56. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

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

2.2.58. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

2.2.59. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

2.2.60. Deve ser possível exportar os logs em CSV;

2.2.61. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

2.2.62. Rotação do log;

2.2.63. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

2.2.64. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação etc.;

2.2.65. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

- **2.2.65.1.** Situação do dispositivo e do cluster;
- **2.2.65.2.** Principais aplicações;
- **2.2.65.3.** Principais aplicações por risco;
- **2.2.65.4.** Administradores autenticados na gerência da plataforma de segurança;
- **2.2.65.5.** Número de sessões simultâneas;
- **2.2.65.6.** Status das interfaces;
- **2.2.65.7.** Uso de CPU;
- **2.2.65.8.** Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
- **2.2.65.9.** Resumo gráfico de aplicações utilizadas;
- **2.2.65.10.** Principais aplicações por utilização de largura de banda de entrada e saída;
- **2.2.65.11.** Principais aplicações por taxa de transferência de bytes;

2.2.65.12. Principais hosts por número de ameaças identificadas;

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

2.2.66. Deve permitir a criação de relatórios personalizados;

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

2.2.68. Gerar alertas automáticos via:

2.2.68.1. Email;

2.2.68.2. SNMP;

2.2.68.3. Syslog;

2.3. ZERO TRUST NETWORK ACCESS (ZTNA) COM CAPACIDADE PARA SUPORTAR 400 USUÁRIOS

2.3.1. REQUISITOS GERAIS DA SOLUÇÃO

2.3.1.1. A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

2.3.1.1.1. ZTNA (Zero Trust Network Access).

2.3.1.1.2. Filtro de URL;

2.3.1.1.3. Controle de Aplicação;

2.3.1.1.4. Prevenção de Ameaças;

2.3.1.1.5. Solução de segurança DNS;

2.3.1.1.6. Proteção Contra Malwares Modernos (Sandbox);

2.3.1.1.7. Gerência e Relatórios.

2.3.1.2. A solução deverá ser licenciada para permitir a autenticação para acesso de 200 usuários conectados simultaneamente

2.3.1.3. A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública e on-premises).

2.3.1.4. A solução deve possuir console única de gestão para toda a plataforma de segurança, incluindo:

2.3.1.4.1. Painel de Política;

2.3.1.4.2. Painel de Relatório;

2.3.1.4.3. Painel de Incidentes;

2.3.1.4.4. Painel de Configuração;

2.3.1.4.5. Painel Analítico.

2.3.1.5. O fabricante da solução deverá possuir ao menos 2 gateways no Brasil com pelo menos 2 (dois) endereços IPs dedicados para cada um deles e garantir que as configurações sejam aplicadas aos mesmos localmente, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

2.3.1.6. A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o Brasil.

2.3.1.7. Esta funcionalidade também deverá garantir que a mesma faixa de endereço não seja compartilhada com outros clientes;

2.3.1.8. Deverá ser fornecida com no mínimo, 2 (duas) estruturas de processamento redundantes no território nacional (Brasil)

2.3.1.9. A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001

2.3.1.10. Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

2.3.1.10.1. Túnel Seguro (IPSEC ou SSL);

2.3.1.10.2. Integração com plataformas de SDWAN;

2.3.1.10.3. Integração com NGFW/UTM (IPSEC);

2.3.1.10.4. Agente (Windows, Linux e MacOS);

2.3.1.11. Os serviços de segurança devem ser fornecidos de maneira transparente às redes/usuários remotas;

2.3.1.12. A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

2.3.1.12.1. Active Directory;

2.3.1.12.2. Federação (SSO) utilizando SAML v2.0.

2.3.1.12.3. OpenID Connect/OAuth 2.0

2.3.1.12.4. Suportar recurso de autenticação única para todo o ambiente, utilizando o padrão de autenticação Active Directory, OpenID Connect/OAuth 2.0 ou outra plataforma com suporte à SAML;

2.3.1.13. A solução deverá ser capaz de prover acesso às aplicações internas sem a necessidade de instalação de máquinas virtuais na rede de destino como ponte de acesso;

2.3.1.14. A solução deverá executar suas funcionalidades para defender a rede/usuário contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

2.3.1.15. A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

2.3.1.16. O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

2.3.1.17. Deverá permitir a configuração de portas diferentes das portas padrão utilizadas pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

2.3.1.18. A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS. Em caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência do TJ-CE, bloquear ou permitir o acesso aos sites;

2.3.1.19. Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

2.3.1.20. O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato;

2.3.2. ZTNA (ZERO TRUST NETWORK ACCESS)

2.3.2.1. A solução deve possuir a capacidade de controlar o acesso e aplicar controle de aplicação, proteção contra malwares modernos (Sandbox), prevenção de ameaças e segurança de DNS, de usuários remotos a aplicações internas através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na

política de segurança e não a um segmento de rede interna;

2.3.2.2. A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

2.3.2.3. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

2.3.2.4. A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

2.3.2.5. Ser possível configurar através da console gráfica da solução quais aplicações internas serão acessadas através do Tenant da solução;

2.3.2.6. Ser autossuficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

2.3.2.7. Trabalhar em modo híbrido, onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters do TJ-CE e nas nuvens públicas indicadas pela mesma;

2.3.2.8. A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows, Linux e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

2.3.2.8.1. Presença de processo(s) em execução;

2.3.2.8.2. Presença de arquivos em disco;

2.3.2.8.3. Participação em domínio do AD;

2.3.2.8.4. Existência de Certificado Digital no dispositivo;

2.3.2.8.5. Que somente as máquinas que estejam com solução anti-malware ativada possam acessar os serviços internos.

2.3.2.8.6. O cliente SSL client-to-site também deve suportar dispositivos móveis (IOS e ANDROID), sistemas operacionais Linux;

2.3.2.9. A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

2.3.2.9.1. Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

2.3.2.9.2. Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada;

2.3.2.10. Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

2.3.2.10.1. Usuário do AD;

2.3.2.10.2. Grupo do AD;

2.3.2.10.3. Aplicação Privada;

2.3.2.10.4. Perfil de segurança (por exemplo: Filtro de URLs, Controle de Aplicação e inspeção Anti-malware);

2.3.2.10.5. Ação: Permitir e/ou Bloquear.

2.3.2.11. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host,

criptografia do disco, chaves de registros e processos ativos;

2.3.2.12. A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido;

2.3.2.13. A confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

2.3.2.14. Possuir capacidade de analisar dinamicamente (continuamente) os acessos dos usuários conectados remotamente a internet e recursos do próprio órgão;

2.3.2.15. Suportar políticas de permissão e negação de acesso com base em várias condições. Por exemplo: postura do dispositivo, localização do dispositivo/usuário, associação ao grupo de usuários;

2.3.2.16. Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

2.3.2.17. A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

2.3.2.17.1. Regra de segurança que foi aplicada no tráfego;

2.3.2.17.2. Ação tomada pela solução;

2.3.2.17.3. Usuário;

2.3.2.17.4. Endereço IP;

2.3.2.17.5. IP público e IP privado.

2.3.2.17.6. País de origem;

2.3.2.17.7. Porta de origem;

2.3.2.17.8. Sistema operacional;

2.3.2.17.9. Aplicação de destino;

2.3.2.17.10. Porta de destino;

2.3.2.17.11. Protocolo;

2.3.2.17.12. Bytes trafegados na sessão;

2.3.2.17.13. Hora de início e término da sessão.

2.3.2.18. Deve permitir que a conexão com o serviço SASE seja estabelecida das seguintes formas:

2.3.2.18.1. Antes do usuário autenticar na estação;

2.3.2.18.2. Após autenticação do usuário na estação;

2.3.2.18.3. Sob demanda do usuário;

2.3.2.18.4. Sempre ativo mantendo o usuário conectado assim que o usuário faz o logon.

2.3.2.18.5. A solução deve enviar a lista de gateways ativos para estabelecimento da conexão;

2.3.2.18.6. Deve haver a opção do cliente remoto escolher manualmente o gateway de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

2.3.3. FILTRO DE URLS

2.3.3.1. A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

2.3.3.2. O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

2.3.3.3. A solução deverá possuir:

2.3.3.3.1. Pelo menos 70 categorias distintas de URLs;

2.3.3.3.2. A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.3.3.3.3. Categoria específica para classificar domínios recém registrados (com menos de 30 dias);

2.3.3.3.4. Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.3.3.4. A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas de filtro de conteúdo WEB:

2.3.3.4.1. Categoria de URL;

2.3.3.4.2. Usuários e Grupos do Active Directory;

2.3.3.4.3. Profile de prevenção de malwares;

2.3.3.4.4. Atividade realizada na URL/Aplicação;

2.3.3.4.5. IP de Origem;

2.3.3.4.6. IP de Destino;

2.3.3.4.7. País de origem e destino;

2.3.3.4.8. Ação: allow, block e alert;

2.3.3.4.9. Tipo de arquivo.

2.3.3.4.10. A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

2.3.3.5. A solução deverá suportar:

2.3.3.5.1. A criação de categorias de URLs customizadas;

2.3.3.5.2. A exclusão de URLs do bloqueio, por categoria;

2.3.3.5.3. A customização de página de bloqueio;

2.3.3.5.4. A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

2.3.3.6. A solução deverá permitir:

2.3.3.6.1. Um mecanismo para sobrescrever as categorias de URL;

2.3.3.6.2. A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

2.3.3.6.3. Especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.3.3.6.4. A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (hit count);

2.3.3.7. A solução deverá possibilitar:

2.3.3.7.1. Categorização e recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.3.3.7.2. A inspeção de tráfego HTTPS Outbound deverá efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

2.3.3.7.3. Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos usuários.

2.3.3.7.4. O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

2.3.3.7.5. 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);

2.3.3.7.6. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

2.3.3.7.7. A solução deverá ser capaz de detectar e prevenir roubo de credenciais, controlando e bloqueando os sites que o usuário pode enviar credenciais corporativas com base na classificação do endereço, em tempo real.

2.3.3.7.8. A solução deverá possuir a capacidade de detectar técnicas de phishing ou falsificação de imagens;

2.3.3.7.9. A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

2.3.4. CONTROLE DE APLICAÇÕES

2.3.4.1. A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.3.4.2. A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

2.3.4.3. Pela solução deverá ser possível:

2.3.4.3.1. A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

2.3.4.3.2. A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

2.3.4.3.3. Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web e interno através da nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

2.3.4.3.4. Adicionar controle de aplicações em todas as regras de segurança da solução, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

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

2.3.4.4. A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

2.3.4.4.1. Nível de risco da aplicação;

2.3.4.4.2. Categoria de aplicações.

2.3.4.4.3. A solução deverá reconhecer pelo menos 3.000 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 webmail;

2.3.4.4.4. A solução deverá suportar múltiplos métodos de

identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

2.3.4.5. A solução deverá diferenciar:

2.3.4.5.1. Tráfegos peer-to-peer (bittorrent, emule, neonet, etc.), possuindo granularidade de controle para os mesmos;

2.3.4.5.2. Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp, telegram e etc.) possuindo granularidade de controle para os mesmos;

2.3.4.5.3. Aplicações proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle para eles.

2.3.4.5.4. A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

2.3.4.6. Pela solução deverá ser possível:

2.3.4.6.1. Inspecionar o payload do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.3.4.6.2. Realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo porta 80 http, buscando por aplicações que potencialmente expõem o ambiente como: peer-to-peer ou mensageiros instantâneos;

2.3.4.6.3. Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como ataques utilizando comunicação TLS;

2.3.4.6.4. Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a encrypted bittorrent e aplicações VOIP que utilizam criptografia proprietária.

2.3.4.6.5. Caso a solução não tenha assinaturas pré-definidas de uma aplicação, ela deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, HTTPS, FTP, E-mail e extensão de arquivos;

2.3.4.6.6. Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

2.3.4.6.7. O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas dele;

2.3.5. PREVENÇÃO DE AMEAÇAS

2.3.5.1. A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

2.3.5.2. Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de cloud storage com nível de risco alto na base do fabricante da solução;

2.3.5.3. Deve conter, no mínimo, as seguintes informações sobre as

aplicações comparadas na interface gráfica da solução:

2.3.5.3.1. Informações sobre vulnerabilidades e exploits já sofridos;

2.3.5.3.2. Certificações e normas que a aplicação está aderente. Ex: PCI, DSS, SOC-1, SOC-2 e SOC-3;

2.3.5.3.3. Informações sobre privacidade de dados. Ex: ao armazenar dados na aplicação, o cliente continua sendo proprietário dos dados.

2.3.5.3.4. A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

2.3.5.4. A solução deverá suportar:

2.3.5.4.1. Várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

2.3.5.4.2. Referência cruzada com CVE.

2.3.5.5. A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

2.3.5.5.1. Domínios de DNS dinâmicos;

2.3.5.5.2. Domínios identificados previamente como sendo distribuidores de Malwares;

2.3.5.5.3. Domínios identificados anteriormente em campanhas de Phishing;

2.3.5.5.4. Domínios identificados previamente como Graywares os quais podem usar de técnicas de instalação de aplicações não desejadas;

2.3.5.5.5. Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

2.3.5.5.6. Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

2.3.5.5.7. A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.3.5.5.8. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

2.3.5.5.9. A solução deverá permitir updates em tempo real para ameaças e novos ataques feitos através de DNS.;

2.3.6. SEGURANÇA DNS

2.3.6.1. A solução de segurança de DNS, tem como finalidade proteger as conexões a domínios maliciosos que muitas vezes são utilizados pelos atacantes, utilizam para interceptar a comunicação e poder ter acesso e controlar a comunicação dos usuários, causando problemas de evasão e exfiltração de dados;

2.3.6.2. Caso o fabricante não tenha solução de segurança para DNS de forma nativa, ou seja, licenciada de forma separada da solução, o mesmo pode compor com outra solução dedicada de mercado de fabricantes como (ex.: Cisco Umbrella) e deverá ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.6.3. A solução de segurança de DNS deve ser capaz de identificar

atividades maliciosas de comando e controle utilizado pelo menos as seguintes técnicas:

2.3.6.4. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.3.6.4.1. Domínio suspeito identificado;

2.3.6.4.2. ID de assinatura de detecção;

2.3.6.4.3. Usuário logado na estação/servidor que originou o tráfego;

2.3.6.4.4. Aplicação;

2.3.6.4.5. Porta de destino;

2.3.6.4.6. IP de origem;

2.3.6.4.7. IP de destino;

2.3.6.4.8. Horário;

2.3.6.4.9. Ação do firewall;

2.3.6.4.10. Severidade;

2.3.6.4.11. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.3.6.5. A análise automática deve incluir, no mínimo, as seguintes características:

2.3.6.5.1. Padrões de consulta;

2.3.6.5.2. Entropia;

2.3.6.5.3. Análise de frequência n-gram de domínios;

2.3.6.5.4. Taxa de consultas.

2.3.6.5.5. A solução deve permitir updates em tempo real para ameaças e novos ataques feitos através de DNS;

2.3.6.5.6. A solução deve permitir a utilização ilimitada (quantidades) de assinaturas DNS;

2.3.6.6. A solução de segurança de DNS deve ser capaz de categorizar os seguintes tipos de domínio:

2.3.6.6.1. Domínios de DNS dinâmicos

2.3.6.6.2. Domínios identificados previamente como sendo distribuidores de malwares

2.3.6.6.3. Domínios registrados recentemente

2.3.6.6.4. Domínios identificados anteriormente em campanhas de phishing

2.3.6.6.5. Domínios identificados previamente como graywares os quais podem usar de técnicas de instalação de aplicações não desejadas

2.3.6.6.6. Domínios Estacionários os quais são sítios com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares.

2.3.6.6.7. Domínio de proxy de animação utilizados com uma forma de driblar a análise de conteúdo.

2.3.7. PROTEÇÃO CONTRA MALWARES MODERNOS

2.3.7.1. A solução deverá possuir nuvem de inteligência proprietária do fabricante que seja responsável em atualizar toda a base de segurança através de assinaturas;

2.3.7.2. A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise em tempo real em uma sandbox, devendo

permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (sandbox). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.7.3. A solução deverá prevenir o uso de exploits avançados;

2.3.7.4. Na solução, a análise deverá prover:

2.3.7.4.1. Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

2.3.7.4.2. Informações sobre as ações do malware na máquina infectada;

2.3.7.4.3. Informações sobre as URLs não confiáveis utilizadas pelo novo malware;

2.3.7.4.4. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

2.3.7.4.5. Detecção de aplicações não confiáveis, utilizadas pelo Malware;

2.3.7.4.6. Assinaturas de antivírus e antispyware de maneira automática.

2.3.7.5. A solução deverá possuir:

2.3.7.5.1. Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS;

2.3.7.5.2. Mecanismo de detecção "antibot", que inclui pelo menos, reputação de endereço IP;

2.3.7.5.3. Funcionalidade de detecção e bloqueio de call-backs.

2.3.7.5.4. A solução deverá prevenir contra ameaças de dia zero:

2.3.7.5.5. Via tráfego de internet;

2.3.7.5.6. Que possam burlar o sistema operacional emulado;

2.3.7.5.7. Através de tecnologias em nível de emulação e código de registro.

2.3.7.5.8. A solução deverá ser capaz de implementar:

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

2.3.7.5.8.2. Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

2.3.7.5.8.3. Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

2.3.7.5.9. A solução deverá suportar ainda:

2.3.7.5.9.1. Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.3.7.5.9.2. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.3.7.5.9.3. Suportar a análise dinâmica de arquivos

maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10, Mac OS X, iOS, Android e Linux;

2.3.7.5.9.4. A solução deve analisar os arquivos do tipo malware em bare-metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;

2.3.8. SUPORTE E GARANTIA DO FABRICANTE

2.3.8.1. O Serviço deverá fornecer:

2.3.8.1.1. Acesso a Especialistas Técnicos e Recursos Online:

2.3.8.1.1.1. A solução deverá fornecer acesso imediato a especialistas técnicos e recursos online, garantindo proteção ao produto oferecido. Os usuários poderão submeter, atualizar e verificar o status dos casos de suporte por meio de um Portal de Suporte ao Cliente online.

2.3.8.2. Transferência de Conhecimento Avançada:

2.3.8.2.1. A solução incluirá uma plataforma completa de transferência de conhecimento. Isso abrangerá documentação detalhada do produto, bancos de dados de resolução de problemas e um ambiente de gerenciamento de casos de suporte baseado em conhecimento, permitindo colaboração entre usuários. Além disso, serão disponibilizados manuais de produtos, guias técnicos, notas de lançamento de software e FAQs para simplificar a resolução de incidentes.

2.3.8.3. Serviço de Melhoria Contínua:

2.3.8.3.1. A solução oferecerá um serviço de melhoria contínua para maximizar o valor do produto. Isso incluirá o desenvolvimento de planos de sucesso personalizados, alinhados com metas e requisitos específicos da organização. Serão realizadas verificações periódicas da saúde da solução e aplicadas as melhores estratégias de utilização para otimização e proteção do investimento.

2.3.8.4. Integração de Fluxos de Trabalho Operacionais:

2.3.8.5. A solução garantirá a integração eficaz com fluxos de trabalho operacionais. A equipe especializada colaborará com a infraestrutura de rede e segurança, identificando pontos de integração, conduzindo verificações regulares e revisões operacionais para promover uma operação mais eficiente e aumentar a confiança na solução.

2.3.8.6. Os SLAs de para tempos de resposta, deverão obedecer aos seguintes níveis de severidade:

Severidade	Descrição	SLA
1	Grave impacto no ambiente de produção, como a perda de dados de produção ou a inoperância de sistemas.	Até 1 hora, contada a partir do registro do chamado.
2	O software opera, porém, seu desempenho em no ambiente de produção é consideravelmente limitado.	Até 2 horas, contadas a partir do registro do chamado.
3	Perda parcial e não crítica de funcionalidade de software no ambiente de produção, mas é viável continuar usando-o por meio de uma	Até 4 horas, contadas a partir do registro do chamado.

	solução alternativa	
4	Questionamento de natureza geral, notificação de discrepância na documentação ou sugestão de aprimoramento ou alteração do produto.	Até 48 horas, contadas a partir do registro do chamado.

2.4. INSTALAÇÃO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.4.1. É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada. Os equipamentos e componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou componente de hardware fora das condições normais recomendadas pelo fabricante.

2.4.2. A Contratada deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off no intuito de revisar os requisitos do projeto, discutir cronogramas de marcos do projeto, membros da equipe e itens de ação de acompanhamento.

2.4.3. Deverá conduzir através de um workshop uma sessão de design profundada do cenário da implantação da solução através da colaboração das principais partes interessadas da contratante no intuito de desenvolver e concordar com os critérios de design e a estratégia de implantação;

2.4.4. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:

2.4.4.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

2.4.4.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

2.4.4.3. Regras de Firewall existentes e aplicáveis à solução ofertada dada a colocação desta na Rede deste parque;

2.4.4.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

2.4.4.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

2.4.4.6. A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos;

2.4.4.7. Aplicação de todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;

2.4.4.8. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

2.4.4.9. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será

considerado entregue, quando for instalado e configurado, com todas as atualizações, configurações e licenças ativadas. Deverão ser adicionados ao Sistema de Gerência Centralizada todos os equipamentos instalados contemplados na solução adquirida. Os equipamentos deverão ser monitorados e gerenciados por este Sistema de Gerência Centralizada;

2.4.4.10. Habilitação das licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução;

2.4.4.11. Inclusão de políticas de segurança encaminhadas pelo CONTRATENTE, pré-existentes em seu ambiente, para os novos equipamentos.

2.4.5. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução, contendo:

2.4.5.1. Os procedimentos de instalação e configuração,

2.4.5.2. Cenário de implantação e integração da rede;

2.4.5.3. Diagrama/documentação de rede para referência;

2.4.5.4. Lista de materiais/inventário da solução;

2.4.5.5. Versão do Sistema Operacional;

2.4.5.6. Hardening/segurança do sistema;

2.4.5.7. Capacidades fundamentais;

2.4.5.8. Requisitos específicos do cenário de implantação;

2.4.5.9. Detalhes de design de baixo nível (por exemplo, endereços IP, nomes de dispositivos, matriz de cabeamento, pesquisa do local, configuração específica do site/dispositivo);

2.4.5.10. Estratégia de validação - principais pontos de verificação a serem testados;

2.4.5.11. Bem como fornecer um repasse sobre a solução e as configurações realizadas.

2.5. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.5.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.1.14, durante todo o período de vigência do contrato.

2.5.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.5.2.1. Suporte técnico para identificação e resolução de problemas em software e hardware;

2.5.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.5.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.5.2.6. Encaminhar incidentes ao fabricante da solução;

2.5.2.7. Suporte em demais configurações de segurança, redundância e

gerência;

2.5.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.5.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.5.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.5.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.5.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.5.2.13. O suporte linguístico fornecido pela contratada deve assegurar que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.5.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.5.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.5.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.5.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.5.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.5.2.19. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.5.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de

Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.5.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

2.5.2.22. A CONTRATADA deverá executar a cada 3 meses e apresentar os resultados encontrados incluindo sugestão de ações de melhoria para serem executadas, Assessments de boas práticas e de revisão de ciclo de vida de segurança, que possam resumir riscos operacionais e de segurança do TJCE, bem como a aderência a melhores práticas e configurações recomendadas pelo fabricante.

2.6. TREINAMENTO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.6.1. Deverá fornecer treinamento para até 8 (oito) alunos, a fim de capacitar os profissionais da CONTRATANTE;

2.6.2. O serviço de capacitação deve consistir na oferta de treinamentos com abordagem prática voltada a todos os requisitos funcionais da solução contratada, tanto relativo a aspectos operacionais, que inclui a utilização prática de todas as principais funcionalidades da ferramenta, como administrativos, que inclui o gerenciamento, suporte e parametrização da solução.

2.6.3. Ministrado por profissionais da CONTRATADA com conhecimentos comprovados na solução oferecida.

2.6.4. Deve incluir fornecimento de documentação didática em papel ou mídia digital com todo o conteúdo.

2.6.5. Deve ser composto por parte teórica e prática, com uso de laboratórios virtuais da CONTRATADA ou do fabricante.

2.6.6. O treinamento deve abordar, no mínimo, os seguintes tópicos:

2.6.6.1. Conceitos, configuração, gerenciamento e diagnóstico de problemas;

2.6.6.2. Arquitetura e Componentes do NGFW;

2.6.6.3. Sistema de Prevenção de Intrusão;

2.6.6.4. Políticas de Segurança e Aplicações;

2.6.6.5. Filtragem de Conteúdo, Aplicações e URL;

2.6.6.6. Balanceamento de Carga e Alta Disponibilidade;

2.6.6.7. Relatórios, Conformidade e Regulamentações;

2.6.6.8. Customização de Relatórios e Monitoramento;

2.6.6.9. Gerenciamento de Usuários e Autenticação;

2.6.6.10. Registros de eventos;

2.6.6.11. Registro de tráfego;

2.6.6.12. Proteção contra Malware;

2.6.6.13. Controle de Acesso e VPN;
2.6.6.14. Balanceamento de Carga e Alta Disponibilidade;
2.6.6.15. Melhores Práticas de Segurança;
2.6.6.16. Atualizações e Manutenção;
2.6.6.17. Teste de Intrusão e Avaliação de Segurança;
2.6.6.18. Backup e Recuperação de Desastres;
2.6.6.19. Integração com Outras Soluções.

2.6.7. A CONTRATADA poderá incluir tópicos e funcionalidades que julgar necessários, além dos elencados acima;

2.6.8. Após o treinamento, a CONTRATADA deve fornecer certificados de participação a cada funcionário participante, incluindo tópicos abordados, duração e instrutores.

2.6.9. Custos de deslocamento, hospedagem e alimentação dos treinandos são de responsabilidade da CONTRATANTE.

2.6.10. A CONTRATADA será o responsável pela preparação do local de treinamento inclusive da disponibilização e instalação de todos os equipamentos.

2.6.11. A duração mínima do treinamento (carga horária) será de 40 (quarenta) horas em 10 (dez) dias;

2.6.12. O curso deverá ser ministrado em língua portuguesa com o material didático utilizado e fornecido preferencialmente em língua portuguesa.

2.7. INSTALAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.7.1. A Contratada deverá realizar a implementação em conjunto com o fabricante realizando a instalação, configuração e funcionamento dos componentes da solução ofertada. Os componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento fora das condições normais recomendadas pelo fabricante.

2.7.2. Este serviço deverá inclui quatro (4) etapas: Implantação, Integração, Repasse de Conhecimento e Documentação;

2.7.3. A Contratada em conjunto com o fabricante deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off para realizar o lançamento inicial do projeto. Esta reunião incluir uma revisão dos requisitos do projeto e uma discussão sobre cronogramas e plano de ação;

2.7.4. Após o kick-off, a Contratada em conjunto com o fabricante deverá gerar um Documento de Requisitos Técnico, baseado no ambiente do cliente

2.7.5. O Documento de Requisitos Técnicos descreverá o ambiente de produção planejado e os procedimentos operacionais;

2.7.6. A Contratada em conjunto com o fabricante deverá:

2.7.6.1. Realizar a configuração com base nos requisitos definidos no Documento de Requisitos Técnicos. As tarefas de configuração devem incluir no mínimo:

2.7.6.1.1. Implantação de usuários móveis;

2.7.6.1.2. Conector ZTNA (Configuração e integração de 4 conectores com até 10 alvos de aplicativos);

2.7.6.1.3. Dez (10) políticas de segurança.

2.7.6.2. Revisar e validar a implantação de acordo com os critérios

definidos no Documento de Requisitos Técnicos, apoiando a integração inicial de usuários móveis e validando o comportamento e a conectividade dos usuários, através de um Teste Piloto de Integração

2.7.6.2.1. No Teste Piloto de Integração deverão ser revisados e os registros de tráfego e ameaças e os fluxos de tráfego e garanta que os usuários possam alcançar os destinos adequados definidos pelas políticas de segurança

2.7.6.3. Realizar uma sessão de transferência de conhecimento após a conclusão dos serviços de planejamento, configuração e validação listados acima;

2.7.6.4. Realiza uma sessão de Transferência de Conhecimento deverá incluir uma descrição do ambiente as-built e uma transferência de conhecimento sobre como gerenciar e operar o ambiente. A transferência de conhecimento deverá ser realizada em uma única sessão de até duas (2) horas, para oito (8) participantes;

2.8. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.8.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.3.8, durante todo o período de vigência do contrato.

2.8.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.8.2.1. Suporte técnico para identificação e resolução de problemas em software;

2.8.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.8.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.8.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos a solução ofertada;

2.8.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.8.2.6. Encaminhar incidentes ao fabricante da solução;

2.8.2.7. Suporte em demais configurações de segurança, redundância e gerência;

2.8.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.8.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.8.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.8.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.8.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.8.2.13. O suporte linguístico fornecido pela contratada deve assegurar

que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.8.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.8.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.8.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.8.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.8.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.8.2.19. A atualização de software quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.8.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.8.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ANEXO II - TERMO DE CIÊNCIA

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no _____ sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no CONTRATANTE.

CIÊNCIA
CONTRATADA – Funcionários

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

Termo de Ciência – TCI

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____,_____ de _____ de 20_____.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ANEXO III - TERMO DE COMPROMISSO – TC

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado em Av. General Afonso Albuquerque Lima, S/N. – Cambeba, Fortaleza-CE CEP:60822-325 – Fone: (85) 3207-7000, CNPJ n° 09.444.530/0001-01, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____, nº _____, _____, _____/__, CEP: __.___-___, CNPJ n° ___.___.___/____-__, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º __/20__ doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da

informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis,

conforme Art. 156 da Lei nº. 14.133/21.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro de Fortaleza-CE, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

Termo de Compromisso

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ Matrícula:	_____ Representante Legal
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ Preposto da Contratada	_____ Fiscal Técnico

_____, _____ de _____ de 20____

ANEXO 2 DO EDITAL – ORÇAMENTO DETALHADO

ID	BEM/SERVIÇO	MODEL/PART NUMBER	QTD.	VLR. UNIT MÉDIO	VLR. TOTAL MÉDIO
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2	R$ 652.367,61	R$ 1.304.735,22
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2	R$ 1.561.136,02	R$ 3.122.272,04
3	GlobalProtect subscription, for device in an HA pair, PA-5410 - 60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2	R$ 482.258,32	R$ 964.516,64
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1	R$ 2.108.798,10	R$ 2.108.798,10
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1	R$ 67.731,11	R$ 67.731,11
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1	R$ 77.022,64	R$ 77.022,64
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2	R$ 562.446,50	R$ 1.124.893,00
8	Implantação da solução de Firewall	-----	1	R$ 17.480,33	R$ 17.480,33

9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	-----	1	R$ 13.440,28	R$ 13.440,28
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	-----	1	R$ 193.740,09	R$ 193.740,09
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade – prazo do contrato: 60 meses	-----	1	R$ 306.231,50	R$ 306.231,50
				VALOR TOTAL GLOBAL	**R$ 9.300.860,95**

OBS 1: O valor constante na coluna “VALOR UNITÁRIO” representa informação ao licitante quanto ao limite MÁXIMO por item, estimado pelo Tribunal, segundo pesquisa de mercado.

OBS 2: Na proposta do licitante deverão ser mantidas as informações constantes nas colunas “ITEM” e “DESCRIÇÃO”, devendo preencher a coluna: “VALOR UNITÁRIO” e “VALOR TOTAL”, com a sua proposta de preços, **observando os limites máximos unitários e totais informados.**

OBS. 3: O **VALOR GLOBAL** refere-se ao **valor máximo da proposta** que deverá ser cadastrada no sistema do Banco do Brasil até a data limite estabelecida no preâmbulo deste Edital.

ANEXO 3 DO EDITAL – MODELO DE APRESENTAÇÃO DA PROPOSTA

Ao
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ
COMISSÃO DE LICITAÇÃO
Ref. PREGÃO N. ____/2024.

Empresa: _____

CNPJ: _____

Endereço/Telefone: _____

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

ID	BEM/SERVIÇO	MODEL/PART NUMBER	QTD.	VLR. UNIT MÉDIO	VLR. TOTAL MÉDIO
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2	R$	R$
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2	R$	R$
3	GlobalProtect subscription, for device in an HA pair, PA-5410 - 60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2	R$	R$
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1	R$	R$
5	Panorama management software, 25 devices	PAN-PRA-25	1	R$	R$

	60 meses – Palo Alto Networks				
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1	R$	R$
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2	R$	R$
8	Implantação da solução de Firewall	-----	1	R$	R$
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	-----	1	R$	R$
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	-----	1	R$	R$
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	-----	1	R$	R$
				VALOR TOTAL GLOBAL	**R$**

Observação:
Emitir em papel que identifique o licitante.

_____ _____
Local e data Assinatura do representante legal da empresa

ANEXO 4 DO EDITAL – MODELO DE DECLARAÇÃO QUE NÃO EXTRAPOLA A RECEITA BRUTA MÁXIMA ADMITIDA PARA FINS DE ENQUADRAMENTO COMO EMPRESA DE PEQUENO PORTE.

PREGÃO ELETRÔNICO N. ____/2024

(PAPEL TIMBRADO DO PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da carteira de identidade nº _____ e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis e sob as penas da lei, ser _____(microempresa e empresa de pequeno porte) nos termos da legislação vigente, e ainda, que os valores somados dos contratos celebrados com a Administração, no ano-calendário de realização da licitação, ainda não atingiram o limite estabelecido, nos termos do **§2, do artigo 4°, da Lei 14.133/21.**

Local e data

Assinatura do licitante/representante legal
(Nome e cargo)

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 5 DO EDITAL – MODELO DE DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

(PAPEL TIMBRADO DO PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da carteira de identidade nº _____ e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis e sob as penas da lei, ser _____(microempresa e empresa de pequeno porte) nos termos da legislação vigente, **não possuindo nenhum dos impedimentos previstos no §4º, do artigo 3º, da Lei Complementar n. 123/2006**.

Local e data

Assinatura do licitante/representante legal
(Nome e cargo)

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 6 DO EDITAL – MODELO DE DECLARAÇÃO DE QUE NÃO EMPREGA MENOR

PREGÃO ELETRÔNICO N. ___/2024

DECLARAÇÃO

....., inscrita no CNPJ n. ....., por intermédio de seu representante legal o(a) Sr(a) ....., portador (a) da Carteira de Identidade n. ..... e do CPF n. ..... DECLARA, para fins do disposto no art. 68, inciso VI da Lei n. 14.133/2021 em harmonia com o inciso XXXIII do art. 7º, da Constituição da República Federativa do Brasil de 1988, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.
Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

(DATA)

.....…
(NOME)

(Observação: em caso afirmativo, assinalar a ressalva acima).

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 7 DO EDITAL – MODELO DE DECLARAÇÃO DE ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

_____(razão social), inscrita com o CNPJ n. _____, por intermédio do seu representante legal _____, portador da Carteira de Identidade n. _____ e do CPF _____, DECLARA, para fins de habilitação no Pregão Eletrônico n. ___/20__, em cumprimento a exigência contida no artigo 63, I, da Lei n. 14.133/2021, aos requisitos de habilitação deste edital. E para os fins do disposto no **subitem 7.1.10** do Edital do Pregão Eletrônico n. __/20__, **declara**, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a a **proposta anexa foi elaborada de maneira independente** [pelo Licitante], e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico n. ____/20__, por qualquer meio ou por qualquer pessoa;

b a intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico n. ____/20__, por qualquer meio ou por qualquer pessoa;

c não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico n. ____/20__ quanto a participar ou não da referida licitação;

d o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a, ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico n. ____/20__ antes da adjudicação do objeto da referida licitação;

e o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do(a) Tribunal de Justiça do Estado do Ceará antes da abertura oficial das propostas; e

f está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Fortaleza, _____ de _____ de 20__.

_____
Empresa Proponente

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 8 DO EDITAL – MODELO DE DECLARAÇÃO PERCENTUAL MÍNIMO DE MÃO DE OBRA CONSTITUÍDO POR MULHERES VÍTIMAS DE VIOLÊNCIA DOMÉSTICA

(DECLARAÇÃO EXIGÍVEL, EXCLUSIVAMENTE, EM LICITAÇÕES DE SERVIÇOS CONTÍNUOS COM REGIME DE DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA)

A empresa _____(razão social), inscrita com o CNPJ n. _____, por intermédio do seu representante legal _____, portador da Carteira de Identidade n. _____ e do CPF _____, **DECLARA**, para fins da contratação de serviços contínuos com regime de dedicação exclusiva de mão de obra, que preenche 8% (oito por cento) das vagas previstas com mulheres vítimas de violência doméstica, nos moldes do art. 3º do Decreto n. 11.430/2023.

_____, em ___de _____ de 20__.

_____
(REPRESENTANTE LEGAL DO LICITANTE NO ÂMBITO DA LICITAÇÃO, COM IDENTIFICAÇÃO COMPLETA)

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 9 DO EDITAL – MODELO DE DECLARAÇÃO DE QUE NÃO POSSUI, EM SUA CADEIA PRODUTIVA, EMPREGADOS EXECUTANDO TRABALHO DEGRADANTE OU FORÇADO

A empresa _____(razão social), inscrita com o CNPJ n. _____, por intermédio do seu representante legal _____, portador da Carteira de Identidade nº _____ e do CPF _____, **DECLARA**, para fins de habilitação no Pregão Eletrônico n. _____/20__, **não possuir, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado**, observando o disposto nos incisos III e IV do art.1º e no inciso III do art. 5º da Constituição Federal.

Fortaleza, _____ de _____ de 20__.

_____
Empresa Proponente

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 10 DO EDITAL – MODELO DE DECLARAÇÃO DE CUMPRIMENTO DE RESERVA DE CARGOS LEGAL PARA PESSOA COM DEFICIÊNCIA OU REABILITADO DA PREVIDÊNCIA SOCIAL

A empresa _____(razão social), inscrita com o CNPJ n. _____, por intermédio do seu representante legal _____, portador da Carteira de Identidade n. _____ e do CPF _____, **DECLARA**, para fins de habilitação no Pregão Eletrônico n. _____/20__, que os serviços por ela produzidos ou prestados **cumprem a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social** bem como atendem às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei n. 8.213, de 24 de julho de 1991.

Fortaleza, _____ de _____ de 20__.

_____
Empresa Proponente

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 11 DO EDITAL – MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS

(PAPEL TIMBRADO DA PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº_____,por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da Carteira de Identidade nº_____e CPF nº _____, DECLARA, sob as sanções administrativas cabíveis, inclusive as criminais e sob as penas da lei, que toda documentação, encaminhada à Comissão Permanente de Contratação do TJCE em meio digital ou físico, é autêntica.

Local e data

Assinatura do representante legal
(Nome e cargo)

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 12 DO EDITAL – MODELO DE DECLARAÇÃO DE QUE AS PROPOSTAS ECONÔMICAS COMPREENDEM A INTEGRALIDADE DOS CUSTOS PARA ATENDIMENTO DOS DIREITOS TRABALHISTAS

(PAPEL TIMBRADO DO PROPONENTE)

DECLARAÇÃO

(nome /razão social) _____, inscrita no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a)_____, portador(a) da carteira de identidade nº _____ e CPF nº _____, considerando o art. 63, §1º da Lei Federal nº 14.133/2021, DECLARA, sob pena de desclassificação, que a proposta econômica compreende 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.

Local e data

Assinatura do licitante/representante legal
(Nome e cargo)

Ao Sr.
Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

ANEXO 13 DO EDITAL – MINUTA DO TERMO DE CONTRATO

CONTRATAÇÃO TEM COMO OBJETO AQUISIÇÃO DE NOVOS APPLIANCES DE PLATAFORMA DE SEGURANÇA EM CLUSTER DE FIREWALLS TIPO CHASSI (NGFW) DA PALO ALTO NETWORKS INCLUINDO LICENÇAS EQUIVALENTES AS SUBSCRIÇÕES EM CURSO, GARANTIA E SUPORTE TÉCNICO PARA ATUALIZAÇÃO DOS FIREWALLS ATUAIS EM PRODUÇÃO PELO PRAZO DE 60 (SESSENTA) MESES, INCLUINDO SERVIÇOS DE INSTALAÇÃO, TREINAMENTO E DEMAIS ESPECIFICAÇÕES E CARACTERÍSTICAS CONSIGNADOS, SOB REGIME DE EMPREITADA POR PREÇO UNITÁRIO, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ E A EMPRESA _____ (PROCESSO ADMINISTRATIVO N. _____).

CT N._____/20__

CÓDIGO DA CONTRATAÇÃO (PAC): TJCESETIN_2024_031

O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ, situado no Centro Administrativo Governador Virgílio Távora, com sede na Avenida General Afonso Albuquerque Lima, S/N, Bairro Cambeba, Fortaleza – CE, inscrito no CNPJ sob o número 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou CONTRATANTE, neste ato representado por seu(sua) Presidente, Des(a). _____ e por seu(sua) Secretário(a) de Tecnologia da Informação, _____, e a empresa _____, representada neste ato por _____, portador da carteira de identidade n._____/___, CPF n. _____, com endereço na _____, inscrita no CNPJ sob o número _____, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei n. 14.133, de 21 de abril de 2021 e pela Resolução n. 169, de 31 de janeiro de 2013, do Conselho Nacional de Justiça, com suas alterações e atualizações posteriores.

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da licitação realizada sob a modalidade Pregão Eletrônico n. ____/2024, devidamente homologada pelo Exmo. Desembargador Presidente do Tribunal de Justiça do Estado do Ceará, tudo em conformidade com as disposições da Lei Nacional n. 14.133/2021, com suas alterações e atualizações posteriores, e o processo administrativo n. _____.

PARÁGRAFO ÚNICO – REGIME DE CONTRATAÇÃO

A execução da presente avença será **indireta**, segundo o regime de execução por **preço unitário**, nos termos dos art. 6°, XXVIII da Lei n. 14.133/21, sendo originário da licitação na modalidade de Pregão, na forma eletrônica, sob o número ____/20__.

CLÁUSULA SEGUNDA – DO OBJETO

O objeto deste Instrumento consiste na ***aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW) da Palo Alto Networks incluindo licenças***

equivalentes as subscrições em curso, garantia e suporte técnico para atualização dos firewalls atuais em produção pelo prazo de 60 (sessenta) meses, incluindo serviços de instalação, treinamento e demais especificações e características consignados, pelo regime de execução indireta, conforme especificações contidas no Edital do Pregão Eletrônico n. ___/2024 e seus anexos, bem como nos Anexos_____ deste Contrato, todos, partes do mesmo.

§ 1º DOCUMENTAÇÃO COMPLEMENTAR

Os documentos constantes do **Processo Administrativo nº. 8509141-65.2024.8.06.0000** integram o presente Termo de Contrato como se nele estivessem transcritos, cujos teores consideram-se conhecidos e acatados pelas partes, sem prejuízos da aplicação de normas técnicas e legislação vigentes relativas ao objeto contratual, especialmente quanto a(ao):

a Termo de Referência;
b Edital e demais anexos do Edital de Pregão Eletrônico nº___/20___; e,
c Proposta da CONTRATADA, no que couber.

§ 2º A prestação dos serviços obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Contrato, no que não o contrarie.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DAS PARTES

São obrigações das partes neste Termo de Contrato:

1 **DO CONTRATANTE**

I Designar formalmente, na forma do art. 177, da Lei nº 14.133/21, representantes para gerenciar e exercer a fiscalização da execução do Contrato, independentemente do acompanhamento e controle exercido pela CONTRATADA.

II Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste contrato, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para o CONTRATANTE.

III Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. Ele deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços/entrega de bens, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

IV Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da CONTRATADA às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas.

V Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com os termos do contrato assinado.

VI Proporcionar todas as condições e prestar as informações necessárias para que a CONTRATADA possa cumprir com suas obrigações, dentro das normas e condições contratuais.

VII Prestar, por meio dos Fiscais Técnicos do Contrato, as informações e os esclarecimentos pertinentes aos serviços/bens avençados, que porventura venham a ser solicitados pela CONTRATADA.

VIII Informar à CONTRATADA sobre atos que possam interferir direta ou indiretamente nos serviços prestados/entrega de bens.

IX Comunicar oficialmente à CONTRATADA, quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

X Registrar e oficializar a CONTRATADA sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

XI Rejeitar, no todo ou em parte, os serviços executados/a entrega de equipamentos que não

atendam às especificações técnicas deste Termo de Contrato.

XII Aprovar ou rejeitar, no todo ou em parte, os serviços executados ou entrega de equipamentos, que não estiverem em conformidade com as especificações constantes da proposta apresentada pela CONTRATADA.

XIII Efetuar o pagamento devido pela prestação dos serviços executados, desde que cumpridas todas as formalidades e exigências avençadas.

XIV Aplicar as sanções previstas em contrato, assegurando à CONTRATADA o contraditório e a ampla defesa.

XV Exigir, sempre que necessário, a apresentação da documentação pela CONTRATADA que comprove a manutenção das condições que ensejaram a sua contratação.

2 DA CONTRATADA

I Manter atualizados seus dados cadastrais junto ao TJCE.

II Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela CONTRATADA, sem ônus adicional ao TJCE.

III Cumprir fielmente os Instrumentos de Medição de Resultados, conforme itens **5.6,5.7**, e demais especificações técnicas do **ANEXO I deste Edital.**

IV Conceder acesso ao TJCE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do TJCE.

V Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJCE, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.

VI Credenciar devidamente um Preposto para representá-lo em todas as questões relativas ao cumprimento dos serviços, de forma a garantir a presteza e a agilidade necessária ao processo decisório e para acompanhar a execução dos serviços e realizar a interface técnica e administrativa com o TJCE e a equipe da CONTRATADA, sem custo adicional.

VII Assumir total responsabilidade pela execução dos serviços/entrega de bens contratados, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.

VIII Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Contrato, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.

IX Comunicar ao TJCE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços/entrega de bens, propondo as ações corretivas necessárias para a execução dos mesmos.

X Submeter ao TJCE qualquer alteração que se tornar essencial à continuação da execução dos serviços/entrega de bens.

XI Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

XII Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.

XIII Selecionar e preparar rigorosamente o(s) empregado(s) que irá(ão) prestar os serviços.

XIV Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência.

XV Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços/entrega de bens.

XVI Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, realizando-os de forma meticulosa e constante, mantendo sempre em perfeita ordem.

XVII Orientar seus empregados de que não poderão se retirar dos prédios ou instalações do

CONTRATANTE portando volumes ou objetos sem a devida autorização e liberação do Fiscal do contrato.

XVIII Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do CONTRATANTE, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

XIX Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento.

XX Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço ou entrega de bens, ou em conexão com ele, ainda que acontecido em dependências do CONTRATANTE.

XXI Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.

XXII Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços ou entrega de bens, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente.

XXIII Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.

XXIV Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua regularização.

XXV Não transferir a outrem, no todo ou em parte, a execução do contrato.

XXVI Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

XXVII Responsabilizar-se pela conduta do empregado que for incompatível com as normas do CONTRATANTE, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação.

XXVIII Receber as observações dos Fiscais Técnicos do contrato, relativamente ao desempenho das atividades/entrega de bens, e identificar as necessidades de melhoria.

XXIX Registrar e controlar, diariamente, as ocorrências e os serviços sob sua responsabilidade.

XXX Permitir a fiscalização e o acompanhamento da execução do objeto deste Termo de Contrato por servidor designado pelo CONTRATANTE, em conformidade com o artigo 117 da Lei nº 14.133/21.

XXXI Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21.

XXXII Indenizar quaisquer danos ou prejuízos causados ao TJCE ou a terceiros, por ação ou omissão do seu pessoal durante a execução dos serviços/entrega de bens.

XXXIII Não colocar à disposição do CONTRATANTE, para o exercício de funções de chefia, pessoal que incidam na vedação dos artigos 1º e 2º da Resolução nº 156/2012 do Conselho Nacional de Justiça (Art. 4º – Resolução 156/2012 – CNJ).

XXXIV Encaminhar para o atesto dos fiscais, as faturas emitidas dos serviços prestados/bens entregues.

XXXV Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais a que o CONTRATANTE for compelido a responder em decorrência desta avença.

XXXVI Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços ou entrega de bens, da relação contratual mantida com o CONTRATANTE.

XXXVII Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

XXXVIII Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.

XXXIX Comprovar vínculo empregatício dos profissionais disponibilizados para prestação dos serviços objeto desta contratação através de Ficha de Registro de Empregado, ou Carteira de Trabalho, ou contrato de prestação de serviço (ou documento similar) ou ainda Contrato Social da empresa, em casos

de vínculo societário.

XL Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Contrato por servidor designado pelo contratante.

XLI Não subcontratar, ceder ou transferir, total ou parcial o objeto desta contratação.

XLII Recrutar e selecionar os profissionais necessários à realização do serviço, de acordo com a qualificação técnica exigida, a ser previamente submetida ao Fiscal para verificação da conformidade.

XLIII Fornecer ao TJCE, ao início da prestação do serviço, a relação nominal dos técnicos que atuarão no cumprimento do objeto contratado, atualizando-a sempre que necessário.

XLIV Tal documentação deverá ser juntada nos autos dos contratos.

XLV Manter atualizada a documentação comprobatória da qualificação dos profissionais alocados na execução do serviço e disponibilizar essa documentação ao Tribunal, sempre que solicitada.

XLVI Manter o TJCE formalmente avisado sobre demissões de profissionais que prestem serviço nas dependências do Tribunal, para fins de cancelamento da autorização de entrada e acessos a recursos, sistemas e aplicativos do TJCE.

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

XLVIII Conceder acesso ao TJCE, o controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do mesmo.

CLÁUSULA QUARTA – DA DESCRIÇÃO DA SOLUÇÃO E DAS ESPECIFICAÇÕES TÉCNICAS

A CONTRATANTE atenderá às especificações e às condições de execução dos serviços, nos termos definidos nesta cláusula.

1 DESCRIÇÃO DA SOLUÇÃO

I Aquisição de solução de alta disponibilidade de Next Generation Firewall com gerenciamento centralizado e integrado, com garantia de funcionamento, atualização de assinaturas de proteção e suporte técnico local ou remoto, no modelo 24x7, pelo prazo de 60 (sessenta) meses; incluindo serviços de instalação e treinamento.

II A solução deve ser composta por dois equipamentos (appliances) que funcionam em cluster, especificamente projetados para atuar como Next Generation Firewall, com hardware e software fornecidos pelo mesmo fabricante.

III Cada equipamento (appliance) integrante da solução de alta disponibilidade deve possuir licença ativada para suportar, de maneira simultânea e integrada, as seguintes funcionalidades: firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), descriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL, controle de transferência de arquivos, roteamento estático e dinâmico, NAT e com garantia durante 60 (sessenta) meses. Devem ser as CARACTERÍSTICAS GERAIS do ANEXO I – ESPECIFICAÇÕES TÉCNICAS deste Edital.

IV A solução de gerenciamento centralizado deverá ser constituída de, no mínimo, um “appliance virtual”, que é uma solução de software baseada em máquina virtual, seguindo os padrões estabelecidos pelo DMTF (Distributed Management Task Force). Alternativamente, poderá ser utilizado um sistema operacional desenvolvido pelo fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual. A instalação da solução de gerenciamento ocorrerá em um ambiente de virtualização e hardware pertencente ao TJCE.

V É obrigatório que todos os equipamentos e seus componentes sejam novos, sem uso prévio, entregues em perfeitas condições de funcionamento e sem quaisquer sinais de danos físicos, tais como marcas, amassados, arranhões ou outras imperfeições. Além disso, devem ser acondicionados em suas embalagens originais.

VI Equipamentos que estejam no fim de sua vida útil ou não recebam mais suporte não serão aceitos.

VII Devido à complexidade das soluções de segurança, faz-se necessário manter um suporte técnico especializado, 24x7, com o objetivo de poder acionar um suporte técnico, obter recomendações de melhores práticas e assessoramento para o funcionamento da plataforma de solução de segurança.

VIII Além disso, a garantia é fundamental para manter contratos de substituição de peças e equipamentos durante a vigência do contrato. Com o objetivo de garantir a continuidade dos serviços e a estabilidade do ambiente, a contratada deverá fornecer um novo hardware, que seja equivalente ou superior, para ser utilizado em situações de falha de equipamento, falha de fabricação, degradação dos serviços ou qualquer outro tipo de problema com a solução. Essa disponibilidade de hardware adicional é crucial para assegurar que o ambiente não seja interrompido ou degradado por tempo indeterminado. A contratada deve estar preparada para lidar prontamente com qualquer eventualidade, minimizando os efeitos adversos sobre o funcionamento do equipamento. A capacidade de resposta rápida e eficiente nessas situações é essencial para manter a integridade e a confiabilidade do ambiente do tribunal, garantindo que as atividades judiciais e administrativas possam ser conduzidas sem interrupções significativas.

2 ESPECIFICAÇÃO TÉCNICA

I Conforme consta no item 4 do **ANEXO I deste EDITAL.**

3 MODELO DE EXECUÇÃO DO OBJETO

I Metodologia de Trabalho

Etapa/Fase/Item	Prazo / Condição
Reunião de alinhamento	Em até 5 (cinco) dias úteis após a data de assinatura do contrato.
Entrega do hardware	Em até 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.
Instalação, configuração e testes da solução	Em até 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.
Operação assistida	Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na tabela do item 1.2, com duração de 20 dias úteis, podendo ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços até que sejam sanadas para o atendimento dos requisitos técnicos.
Treinamento	Está condicionada à solicitação prévia, via emissão de ordem de serviço por parte da Contratante, em data a ser previamente acordada com o TJCE.
Documentação	Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço.
Período de suporte, monitoramento e garantia da solução de TI	60 (sessenta) meses após a emissão do Termo de Recebimento Definitivo.
Regime para atendimento da garantia on-site	NBD - Next Business Day (próximo dia útil) em atendimento

	no regime 24x7 (24 horas por dia, 7 dias na semana)

Etapa	Método
Entrega do Objeto	**01 (hum) Appliance de Firewall deverá ser entregue**: TJCE – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325, prédio ANEXO – Centro de Documentação e Informática (CDI) – Secretaria de Tecnologia da Informação/Departamento de Infraestrutura de TI. **01 (hum) Appliance de Firewall deverá ser entregue**: Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza - CE, 60811-690.Deverá ser conferido as quantidades por item.
Recebimento Provisório e Recebimento Definitivo	Quando da entrega do objeto do contrato, os equipamentos serão avaliados quanto as suas características técnicas, a fim de se verificar a conformidade com àquelas exigidas no Termo de Referência. Será também avaliado o tempo de fornecimento da solução dentro dos prazos especificados, que no caso da entrega do objeto, é de até 30 (trinta) dias corridos contados da data de emissão da Ordem de Fornecimento de Bens. O recebimento definitivo da solução de TI fornecida ocorrerá após recebimento e conclusão da etapa de " Instalação, configuração e testes da solução", por parte da Contratante, da conformidade do produto ofertado quanto às exigências contidas no Termo de Referência em até 10 (dez) dias corridos, contados da data de emissão do Termo de Recebimento Provisório.
Durante a Garantia	Durante a prestação da garantia, será avaliado o cumprimento dos prazos de solução dos chamados e a conformidade técnica dos equipamentos substituídos.

II A execução do objeto deve incluir as fases de planejamento, instalação, configuração, migração tecnológica, elaboração de documentação técnica e operação assistida. Tais fases devem observar as seguintes condições:

a Condições Gerais

i A CONTRATADA é responsável por realizar as seguintes atividades, em conformidade com as especificações técnicas de cada item, apresentadas e aprovadas previamente pelo TJCE:

1º.) Planejamento, instalação, configuração e migração tecnológica.

2º) Elaboração de documentação técnica.

3°) Operação assistida dos serviços.

ii. Estas atividades também abrangem o levantamento da solução atualmente em uso no Tribunal e a migração das configurações existentes para o ambiente proposto.

iii. Desde o início das atividades referentes à fase de planejamento até o recebimento definitivo de cada item de serviço, a CONTRATADA deve alocar profissionais com experiência comprovada na tecnologia dos produtos para cada um dos serviços.

iv Da mesma maneira, a CONTRATADA deve manter profissional com papel de gerente de projeto para realização das atividades de planejamento, interlocução, elaboração de cronograma e entrega de documentação técnica associada à fase.

b Etapas

i Os Serviços Gerenciados de Segurança devem ser entregues em etapas:

1º) Reunião de alinhamento

2º) Entrega de hardware

3°) Instalação, configuração e testes das soluções

4°) Operação assistida

5º) Treinamento
6º) Documentação

c Reunião de alinhamento

i. Em até 5 (cinco) dias úteis após a data de assinatura do contrato, deverá ser realizada reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e Anexos, bem como o planejamento e definições de roteiro de suporte técnico dedicado, e esclarecer possíveis dúvidas acerca da execução dos serviços.

ii. O Plano de Implantação deverá ser alinhado na reunião de kick-off, juntamente com a equipe técnica da SETIN.

iii. Deverão participar dessa reunião, no mínimo, os fiscais do contrato, o Preposto da Contratada e demais intervenientes necessários. Caso a contratante entenda que seja necessária a presença do fabricante, o mesmo deverá estar presente na call de Kick-off.

iv. A reunião deverá ocorrer no TJCE ou por vídeo conferência, de preferência, antes do início da execução dos serviços / entrega dos bens, em data e horário a ser agendada pelos fiscais do contrato.

v. Nessa reunião, a Contratada deverá apresentar oficialmente seu Preposto, além da equipe técnica responsável pelo atendimento do serviço especializado e suas respectivas qualificações técnicas.

vi. Será realizada, na reunião, o alinhamento dos aspectos principais para o Plano de Implantação que deverá ser entregue pela Contratada, idealizada por ambas as partes.

vii. A Contratada deverá apresentar um número de telefone que possibilite ligações para a central de suporte, portal/url e endereço de e-mail para fins de abertura, acompanhamento de chamados e resolução de dúvidas sobre a Solução;

viii. Os profissionais indicados pela Contratada deverão efetivamente atender os serviços objeto do contrato, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo TJCE.

ix. A Contratada cumprirá as instruções complementares do TJCE quanto à execução e horário de realização do serviço, permanência e circulação de seu(s) técnico(s) nas dependências do TJCE.

d Entrega do hardware

i. Após a assinatura do contrato, os fiscais do contrato ficarão aptos a solicitar o primeiro empenho.

ii. A entrega dos equipamentos deverá ocorrer em, no máximo, 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.

iii. Os equipamentos e componentes serão entregues pela CONTRATADA em perfeitas condições de operação, salvo quando ocorrerem situações fora do controle da mesma, tais como: greves nos serviços de transportes, guerras e perturbações de caráter social, político ou econômico, devidamente comprovadas e formalmente aceitas pelo TJCE.

iv. Os equipamentos e materiais deverão ser entregues acondicionados adequadamente, em caixa lacrada, de forma a resistir à armazenagem e permitir completa segurança durante o transporte.

v. A entrega deverá ocorrer no horário das 08:00 às 17:00, de segunda a sexta-feira, exceto nos feriados nos seguintes endereços:

1º) 01 (hum) Appliance de Firewall deverá ser entregue: TJCE – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325, prédio ANEXO – Centro de Documentação e Informática (CDI) – Secretaria de Tecnologia da Informação/Departamento de Infraestrutura de TI.

2°) 01 (hum) Appliance de Firewall deverá ser entregue: Fórum Clóvis Beviláqua, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza – CE, 60811-690.

vi. O não cumprimento do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada, implicará as sanções administrativas previstas neste termo de referência.

vii. A CONTRATADA deverá informar ao TJCE a disponibilidade do produto para que sejam tomadas todas as providências necessárias ao início da execução do teste de recebimento

definitivo, a ser efetuado.
viii. Entende-se como recebimento definitivo dos produtos, aquele recebido funcionando e em perfeitas condições, com a devida instalação, quando esta estiver prevista nas especificações.
ix. Por ocasião do recebimento definitivo dos produtos será assinado documento pertinente, que integrará o Contrato.
x. Juntamente a cada produto entregue deverão constar os respectivos manuais de instruções e demais literaturas técnicas pertinentes, bem como respectivas notas fiscais e/ou faturas.
xi. Caberá à Contratada a responsabilidade pela entrega dos bens, com todas as despesas de transporte, frete e seguro correspondentes;
xii. O material deverá ser entregue pela Contratada em perfeitas condições de operação;
xiii. Deverá ser entregue, juntamente com os bens adquiridos, as respectivas notas fiscais e/ou faturas.
xiv. Por ocasião do recebimento provisório/definitivo dos produtos, será assinado documento pertinente, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021.
xv. Sendo necessário o pedido de prorrogação de prazo para entrega dos materiais, somente será conhecido por este Tribunal caso tal pleito seja devidamente fundamentado e protocolado de maneira virtual, juntamente com documentação probatória das alegações, no e-mail dos fiscais do contrato, em até 05 (cinco dias) antes de expirar o prazo inicialmente estabelecido.
xvi. A garantia dos equipamentos e o serviço de suporte técnico iniciarão após a emissão do Termo de Recebimento Definitivo.
xvii. Constatado defeito de fábrica do material, cabos e módulos, em sua utilização durante o prazo de garantia do produto, a Contratada deverá substituí-los por outros iguais ou superiores, no prazo de dez (10) dias úteis contados a partir da notificação efetuada pelo Contratante, sem qualquer ônus adicional.
xviii A garantia on-site dos equipamentos deverá ser realizada nos Data Centers do Tribunal de Justiça.

e Instalação, configuração e testes das soluções

i. A execução dos serviços de instalação, configuração e disponibilização dos licenciamentos deverá ocorrer em, no máximo 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.
ii. A CONTRATADA deverá entregar, em até 02 (dois) dias úteis após a conclusão da instalação dos equipamentos, relatório de instalação que deverá conter: confirmação de todos os equipamentos e perfeito funcionamento do hardware, identificação de cada produto instalado (marca, modelo, versão, número de série, número da licença, etc.), nome, matrícula, data e assinatura do técnico responsável pela CONTRATADA e do técnico do TJCE.
iii. A CONTRATADA deve ser responsável por prover os recursos necessários à instalação e configuração de equipamentos, sem ônus adicionais ao Tribunal, incluindo o fornecimento de cabos elétricos, cabos lógicos, adaptadores elétricos, parafusos, porcas, conectores, kits racks, tomadas e demais materiais necessários à instalação de equipamentos nos locais de prestação dos serviços, incluindo o fornecimento de transceivers/transceptores para a utilização de interfaces de fibra-óptica.
iv.Caberá a CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no local da instalação dos equipamentos, bem como pela retirada e entrega dos mesmos, de peças de reposição e componentes necessários, com todas as despesas de transporte, frete e seguros correspondentes.
v. Além dos recursos de infraestrutura supracitados, a CONTRATADA deve ser responsável pelo fornecimento de licenças de sistemas operacionais, quando necessários para o provimento dos softwares integrantes da solução proposta. Nesse contexto, incluem-se sistemas operacionais básicos, patches de atualização, softwares de aplicações, softwares de bancos de dados, entre outros.
vi. Ademais, os equipamentos e softwares necessários à prestação dos serviços devem estar cobertos por contratos de suporte técnico e garantia do fabricante durante o período de vigência de cada um dos itens de serviço.
vii. Os softwares propostos e licenciados para a solução, excluindo aqueles a serem instalados

em equipamentos para o provimento de serviços integrados, quando explicitamente permitidos, devem ser instalados em máquinas virtuais a serem providas pelo TJCE. Nesse contexto, incluem-se os softwares dimensionados para prover diretamente serviços da solução, bem como aqueles referentes à administração e monitoramento de equipamentos e serviços, que devem ser instalados em sua última versão estável e atualizada pelos respectivos fabricantes.

viii. Ademais, os equipamentos e softwares devem ser integrados à base de usuários com privilégios administrativos do Microsoft Active Directory e RADIUS (Remote Authentication Dial-in User Service) da rede do Tribunal para concessão de perfis de acesso às ferramentas implementadas. Nesse contexto, devem ser configurados 3 (três) perfis de acesso para os serviços: um perfil de leitura, consulta a informações, configurações e logs, para o acompanhamento da execução de serviços por parte da equipe técnica do TJCE; um perfil de controle total para a execução das atividades de administração e gerência remota da plataforma por parte da CONTRATADA; e um terceiro de controle total para a execução das atividades de administração e gerência da plataforma por parte da equipe técnica do TJCE, a ser utilizada somente em caso de grave emergência, como nos casos de sinistros que causem a indisponibilidade total dos serviços ou a indisponibilidade da CONTRATADA. Essas credenciais de acesso, para uso em caso de emergência, devem ser armazenadas em cofre do Tribunal, cujo procedimento de utilização deve ser acordado com a CONTRATADA em momento oportuno.

ix. Todos os elementos instalados devem ser configurados para envio de logs para a solução de consolidação e correlacionamento de eventos do Tribunal, implantada em ambiente virtualizado, responsável pela coleta, processamento, normalização, armazenamento e correlação de eventos gerados pelos diversos servidores de rede e de aplicação. Dessa forma, as atividades de levantamento, desenvolvimento de conectores e implantação de casos de uso de correlacionamento da solução implantada deve fazer parte das etapas de implantação da solução.

x. Além disso, os equipamentos e softwares fornecidos devem ser configurados para enviar notificações e alarmes de performance e disponibilidades ao software de monitoramento adotado e implantado na infraestrutura do TJCE.

xi. Faz parte da fase de instalação a interação com as equipes do TJCE para configuração das rotinas de backup da solução ofertada e da realização de testes de restore e de desligamento/religamento da solução.

xii. Finalmente, todas as regras, configurações e serviços existentes na solução de segurança atualmente instalada no TJCE devem ser avaliadas e os elementos instalados devem ser configurados de forma a compatibilizar tudo com os ajustes necessários para melhoria e otimização, de forma a garantir nível de segurança igual ou superior.

xiii. O licenciamento de uso e a execução dos serviços de suporte técnico e garantia deverão ser iniciadas com base na data de recebimento definitivo dos seus respectivos equipamentos.

xiv. A garantia dos equipamentos e software terá vigência de 60 (sessenta) meses contados da data dos respectivos recebimentos definitivos e para os itens que envolvem entrega de novos equipamentos.

f Operação assistida

i. Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na **tabela do item 1.2 do Anexo I deste Edital.**

ii. A operação assistida deve ter a duração de 20 dias úteis, de modo a assegurar a execução de ações rápidas corretivas necessárias ao bom funcionamento dos serviços e reduzir riscos inerentes à migração tecnológica da plataforma atualmente existente.

iii.As atividades de operação assistida devem ser realizadas obrigatoriamente com a presença de técnico capacitado, em horário comercial, e devem se iniciar logo após a migração tecnológica, testes e ativação dos serviços. Caso seja necessária a consecução de atividades que possam afetar a disponibilidade dos serviços, as atividades de operação assistida podem ser prolongadas após o horário comercial, sem qualquer ônus para o TJCE.

iv. A duração das atividades de operação assistida pode ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços

até que sejam sanadas para o atendimento dos requisitos técnicos.

v. O período de operação assistida deve englobar, entre outras, as seguintes atividades para cada um dos itens de serviço:

1º) Monitoramento de funcionamento e da capacidade dos serviços, resolução de problemas (troubleshooting), análise da efetividade de regras e configurações, simulação de abertura de chamados, instalação de patches, execução/revisão de procedimentos de backup e restore de configurações, definição de casos de uso para correlacionar eventos, manutenção da documentação técnica e revisão de boletins e indicadores;

g Treinamento

i. A prestação dos serviços relacionados ao item de Treinamento – está condicionada à solicitação prévia, por uma ordem de serviço, em data a ser previamente acordada com o TJCE.

ii. A alteração dos prazos para início e término de uma Ordem de Serviço somente deve ser possível mediante apresentação tempestiva de justificativas plausíveis, a serem analisadas e devidamente aceitas pelo Tribunal.

h **Documentação**

i. Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço, contendo as seguintes informações:

1º) Descrição dos serviços implantados, assim como os procedimentos de instalação e configuração;

2º) Descrição da topologia física de equipamentos após a ativação dos serviços e o cenário de implantação e integração da rede;

3º) Descrição de topologia lógica e detalhes de design de baixo nível (por exemplo, endereços IP, nomes de dispositivos, matriz de cabeamento, pesquisa do local, configuração específica do site/dispositivo);

4º) Dados dos equipamentos e softwares, incluindo configurações, números de série e versões;

5º) Parâmetros de configuração, operação, instalação, manutenção, atualização e correto funcionamento dos equipamentos e softwares;

6°) Hardening/segurança do sistema;

7º) Definição de responsabilidades;

8°) Recursos de alta disponibilidade;

9°) Scripts de operação, incluindo desligamento e ligamento, switch over, acionamento do equipamento de contingência, quando necessário;

10º) Procedimentos para abertura e atendimento a chamados;

11°) Procedimentos de recuperação de equipamentos;

12°) Rotinas de backup e restore dos equipamentos, softwares e configurações implantadas;

13°) Rotinas periódicas configuradas;

14°) Desenho dos racks onde estão instalados os equipamentos (bayface);

15º) Definição de padrões porventura existentes na solução (ex. padrão de nome de objetos)

16°) Documentação das informações de configuração cadastradas.

III Instrumentos de Solicitação do Serviço de Suporte Técnico e Monitoramento

a Abertura em central de atendimento único para todos os serviços;

b Serão utilizados os seguintes instrumentos formais de solicitação do(s) serviço(s):

1º) Atendimento através de canal telefônico gratuito 0800 ou com custo de ligação local em Fortaleza/CE, 24x7 (vinte e quatro horas por dia, sete dias por semana);

2°) Chamado técnico através de site na Internet da CONTRATADA, 24x7 (vinte e quatro horas por dia, sete dias por semana), e/ou canal telefônico gratuito 0800 ou custo de ligação local para Fortaleza/CE;

c No provimento deste serviço por meio de telefone (0800), a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

d Para os atendimentos por meio de telefone (0800) ou de Call Center, o tempo máximo de espera deverá ser de até 03 (três) minutos.

e No caso de a CONTRATADA optar pelo atendimento por Website, deverá ser possível que ao TJCE indique uma lista de produtos por meio de arquivo anexo ou diretamente na página, em um único

registro. Neste caso, a data e hora do registro serão consideradas como horário da abertura do chamado para todos os produtos listados.

f A CONTRATADA deverá permitir que o TJCE acompanhe o estado de chamados abertos no Centro de Assistência Técnica do fabricante por meio de site da Internet. O acesso ao Centro de Assistência Técnica deverá estar disponível durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, passível de penalidade em caso de descumprimento, conforme disposto no item **11** do ANEXO I deste Edital.

g O horário de abertura de chamado será determinado conforme abaixo:

1°) Para chamados abertos pelos canais 0800 ou Call Center → o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional do TJCE informando do problema ocorrido. Caso a atendente não possa informar o número e chamado neste momento, a mesma deverá, obrigatoriamente, informar um número de protocolo que registre a data e hora da ligação realizada.

2°) Para chamados abertos pelo canal Website → o horário da abertura do chamado será a data e hora do acesso ao Website para registro do problema ocorrido. No momento do registro, a página web deverá informar o número de chamado. Caso isso não seja possível, a mesma deverá informar um número de protocolo que registre a data e hora do acesso realizado.

h O horário de abertura do chamado demarcará o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA. O horário de abertura de chamado será determinado conforme descrito no subitem 5.3.7 do ANEXO I deste Edital.

i O horário de abertura do chamado demarcará o início da contagem do prazo de retorno, para os chamados estabelecidos como severidade 4, independente do retorno da CONTRATADA. O horário de abertura de chamado será determinado conforme descrito no subitem 5.3.7 do ANEXO I deste Edital.

j Não deverá haver qualquer limitação para o número de técnicos do TJCE autorizados a abrir chamados técnicos.

IV Local de Execução do Serviço

a A execução dos serviços, assim como a instalação dos equipamentos deverá ocorrer nos seguintes endereços, após agendamento prévio com os fiscais do contrato:

1°) **Tribunal de Justiça do Estado do Ceará**, situado na Av. General Afonso Albuquerque Lima, S/N. - Cambeba CEP: 60822-325.

2°) **Fórum Clóvis Beviláqua**, situado na Rua. Des. Floriano Benevides Magalhães, 220 – Edson Queiroz, Fortaleza – CE, 60811-690.

V Horário de Execução do Serviço

a A prestação dos serviços presenciais de suporte técnico, instalação e configuração dos equipamentos de verão ocorre normalmente de segunda a sexta-feira, das 8h às 18h, a menos que haja um acordo prévio entre as partes. Em casos de execução de garantia, substituição de hardware ou emergências que exijam atendimento 24 horas por dia, 7 dias por semana, o serviço será disponibilizado mediante acordo prévio.

b Os serviços serão solicitados mediante a abertura de um “chamado”, efetuado por técnicos do Contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português – para o horário comercial – horário oficial de Brasília).

c Para entrega, instalação e configuração dos equipamentos, deverá seguir agendamento prévio com os fiscais do contrato.

d **Relatório de Instrumento de Medição de Resultados:** Relatório elaborado mensalmente pela Contratada e encaminhado via e-mail aos fiscais do contrato, contendo, no mínimo, as seguintes informações:

1º) Contratante;
2º) Número do Contrato;
3º) Endereço;
4º) Mês de Referência;
5º) Data da realização;
6º) Data de registro do chamado, início e fim do atendimento;
7º) Fiscal técnico responsável;
8º) Responsável técnico da Contratada;

e A Contratante possui ampla liberdade de contestar os dados informados no Relatório de Instrumento de Medição de Resultados, podendo solicitar correções no mesmo, no prazo de 3 (três) dias úteis, caso identifique que as informações apresentadas estejam incorretas.

f Após a análise e aprovação deste relatório, a Contratante deverá emitir o documento "Autorização para Faturamento", descrito no item 5.5.7 do ANEXO I deste Edital.

g Autorização para Faturamento: Autorização emitida pelo Fiscal Administrativo do Contrato ao Preposto da Contratada. Este documento contém a autorização para que a Contratada possa efetuar o faturamento.

VI Instrumento de Medição de Resultados – IMR

a A prestação do Serviço Técnico executado terá sua qualidade medida por meio de Instrumento de Medição de Resultados – IMR.

b Havendo qualquer interrupção ou mal funcionamento da solução, o TJCE efetuará abertura de chamado reportando todos os sintomas.

c Serão considerados para efeitos de medição de resultados:

1.º) Prazo de Atendimento: Tempo decorrido entre a abertura do chamado técnico efetuado pelo TJCE na Central de Atendimento do Contratado e o efetivo início dos trabalhos de suporte.

2.º) Prazo de Solução Definitiva: Tempo decorrido entre a abertura do chamado técnico efetuado pela SETIN na Central de Atendimento do Contratado e a efetiva recolocação da solução em pleno estado de funcionamento.

d A contagem do prazo de solução definitiva de cada chamado será a partir da abertura do chamado técnico na Central de Atendimento disponibilizado pelo Contratado, até o momento da comunicação da solução definitiva do problema e aceite pela SETIN.

e As características do serviço IMR são as seguintes:

1.º) Horário Comercial de Atendimento: 08h às 18h, de segunda a sexta-feira;

2.º) Tempo de solução: varia de acordo com a severidade;

3.º) O prazo de solução poderá ser prorrogado, de acordo com as tratativas do atendimento, mediante aprovação prévia dos fiscais do contrato;

4.º) Em casos comprovados em que a resolução da solução dependa exclusivamente do fabricante, o prazo poderá ser prorrogado, conforme definido entre os fiscais e a empresa contratada;

5.º) Intervalo de cobertura: 24 x 7 (24 horas por dia, 7 dias por semana)

6.º) Suporte a distância/remoto: Assistência remota para solução de problemas comuns de suporte.

7.º) Todo e qualquer procedimento de atualização remota deve ser programado, previamente, entre a CONTRATADA e os fiscais do contrato, através de e-mail.

VII Indicadores de Instrumento de Medição de Resultados – IMR

a Os Indicadores do Instrumento de Medição de Resultados (IMR) serão elencados para os serviços de suporte técnico da solução.

b Os serviços serão medidos, controlados e acompanhados pela Contratante durante o período de vigência do contrato, assim como a definição do Instrumento de Medição do Resultado (IMR), com os acordos de níveis de serviço desejado e suas respectivas notificações ou penalidades.

c O principal elemento para medir a qualidade e a eficácia dos serviços prestados pela Contratada será o IMR. Com relação a esse item, serão considerados os seguintes aspectos:

1.º) O IMR será aplicado a todos os serviços prestados pela Contratada indicados nesse tópico e não por amostragem.

2.º) Objetivando a qualidade, a Contratada deverá estabelecer procedimentos e condições que permitam a melhoria contínua dos serviços prestados.

3.º) As medições dos indicadores de nível de serviço serão aferidas pelos fiscais do contrato.

4.º) O não cumprimento de um ou mais indicadores do IMR ocasionará a aplicação de notificação ou penalidades à Contratada previstas em contrato.

5.º) A Contratante poderá avaliar as justificativas fundamentadas apresentadas pela Contratada para não aplicação das notificações ou penalidades.

d Ao abrir um chamado relativo ao serviço de suporte técnico, o Contratante poderá classificá-lo em 4 (quatro) níveis de severidade:

1.º) Severidade 1: quando ocorre a paralisação dos sistemas objeto desta contratação, configurando-se como situação de emergência.

2.º) Severidade 2: quando se verifica uma grave perda de funcionalidades em programas ou sistemas do TJCE, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço;

3.º) Severidade 3: quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas do TJCE, causando apenas inconveniências para a devida prestação dos serviços pelo TJCE;

4.º) Severidade 4: quando se verifica como necessária a prestação de suporte local proativo para orientação e apoio às melhores práticas para análise do ambiente, execução de implementações visando melhorias na arquitetura, integrações, capacidade, desempenho e elaboração de relatórios executivos, gerenciais e operacionais, sem que haja indisponibilidade e/ou perda de funcionalidades dos sistemas do TJCE, incluindo a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas.

e A Contratada deverá respeitar os seguintes Instrumentos de Medição de Resultados para o suporte técnico da solução, consoante cada indicador do IMR:

Prazo máximo para solução definitiva, ou apresentação de solução de contorno.	
Chamados de Severidade 1	Até 4 Horas, contados a partir do registro do chamado.
Comprometimento para início do atendimento e resposta	
Chamados de Severidade 2	Até 30 Minutos, contados a partir do registro do chamado.
Chamados de Severidade 3	Até 2 Horas, contados a partir do registro do chamado.
Chamados de Severidade 4	Até 4 Horas, contados a partir do registro do chamado.
Ferramentas de Suporte	
Últimos Hot Fixes e Service Packs	Sim
Grandes Upgrades e Melhorias	Sim
Acesso a fóruns de produtos da Fabricante	Acesso Total
Acesso a Base de Conhecimento de Suporte On-Line	Especialista
Suporte de Hardware	
Determinação de RMA – Autorização para devolução de material	Parceiro
Método de envio RMA – Autorização para devolução de material	Próximo vôo / Express Delivery (quando aplicável) ou Envio no Mesmo Dia Útil.

f O nível de severidade será atribuído pelo TJCE no momento da abertura do chamado.
g Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento.
h Toda e qualquer despesa decorrente do suporte remoto ou "on site" desses atendimentos serão de responsabilidade da CONTRATADA.
i No atendimento dos chamados, para efeitos de apuração do tempo gasto pela CONTRATADA para a Disponibilização da Solução, serão desconsiderados os períodos em que o TJCE estiver responsável por executar ações necessárias para a análise e solução da ocorrência.
j Em quaisquer casos e quando necessário, a CONTRATADA deverá enviar informações, para o e-mail dos fiscais técnicos, sobre as correções a serem aplicadas.
k Caso não haja manifestação da CONTRATADA dentro do prazo definido **no item VII, letra "e"** ou caso o Fiscal do Contrato entenda ser improcedente a justificativa apresentada, será iniciado processo de sugestão de aplicação de penalidades previstas, conforme o IMR transgredido.
l Após a conclusão do suporte, a Contratada comunicará o fato aos fiscais do contrato e solicitará autorização para o fechamento do chamado. Caso o mesmo não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Nesse caso os fiscais do contrato informarão as pendências relativas ao chamado aberto.
m Sempre que houver quebra dos IMR, o(s) fiscal(is) técnico(s) emitirá(ão) notificação a Contratada, ou seu preposto, que terá o prazo de, no máximo, 05 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.
n Caso não sejam observados os prazos para atendimento previstos, ou ainda se a justificativa apresentada não for aceita pelos fiscais responsáveis do Contrato, a Contratada estará sujeita a multas/glosas, calculadas sobre o valor descrito mensal do contrato.
o A solução deverá realizar upload de logs (diagnósticos) pelo sistema, para o fabricante, de forma a permitir diagnósticos mais eficazes.
p Ao final de cada mês, a CONTRATANTE avaliará o cumprimento, pela Contratada, dos IMR, conforme **no item VII, letra "e" desta cláusula.**
q Caso haja descumprimento dos IMR, por problemas alheios à CONTRATANTE, e se as justificativas apresentadas pela Contratada forem consideradas insuficientes pela fiscalização, será aplicado desconto à fatura mensal do serviço de atualização e supor-te técnico das subscrições, conforme o disposto abaixo:

SEVERIDADE	DESCRIÇÃO	PENALIDADE
1	Prazo de Solução	Glosa de 20% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 5% sobre o valor da fatura mensal do serviço a cada dia de atraso.
2	Prazo de Solução	Glosa de 10% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 2,5% sobre o valor da fatura mensal do serviço a cada dia de atraso.
3	Prazo de Solução	Glosa de 5% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 1% sobre o valor da fatura mensal do serviço a cada 2(dois) dias de atraso.

4	Prazo de Solução	Glosa de 2,5% sobre o valor da fatura mensal do serviço, aplicada em dobro na sua reincidência. Soma-se glosa de 0,5% sobre o valor da fatura mensal do serviço a cada 3(três) dias de atraso.

r A aplicação das glosas acima descritas estará restrita ao máximo de 02 (duas) ocorrências (chamados técnicos), podendo ser acumulado os valores de multa quando alterado a severidade pelos fiscais do contrato, durante a vigência do contrato.

s A CONTRATADA ficará sujeita às penalidades previstas no **item VII, letra "q"**, sem prejuízo das Sanções Administrativas constante nesse **Edital.**

t O atraso no prazo de solução, de qualquer severidade disposta no **item VII, letra "e"**, superior a 25 (vinte e cinco) dias ou após 02 (duas) ocorrências (chamados técnicos) - **item VII, letra "r"** – autoriza a Administração aplicar as sanções previstas no **item 11 do ANEXO I deste Edital** e se for o caso, promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem o inciso I do art. 137 da Lei n. 14.133 de 2021.

u As penalidades previstas neste Termo de Referência não excluem aquelas dispostas na Lei nº 14.133/21 Art. 156 e 162.

VIII Das considerações acerca das soluções de contorno

a Considerando que a solução das ocorrências de substituição de equipamentos, pela sua natureza, pode envolver atividades relacionadas importação de procedimentos alfandegários, admite-se para todos os casos a adoção de solução de contorno, respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível. Neste caso, a partir do encerramento do chamado original com a disponibilização da solução de contorno, deverá ser imediatamente aberta uma nova ocorrência para provimento da solução definitiva, na qual deverá constar, obrigatoriamente, um novo campo contendo o número do chamado original (encerrado com a solução de contorno, mais Severidade).

b A solução de contorno não deverá utilizar-se de tempo superior a 50% (cinquenta por cento) do prazo definido para a severidade do qual o chamado está sendo executado.

IX O prazo máximo para disponibilização da solução definitiva será:

Prazos para solução definitiva (a partir do encerramento do chamado original, com a disponibilização da solução de contorno)	
Severidade Informada	**Tempo para solução**
1	15 dias corridos
2	20 dias corridos
3	30 dias corridos
4	Conforme agendamento

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

b Em caso de impossibilidade da disponibilização de solução de contorno ou definitiva, dentro dos prazos estabelecidos, a CONTRATADA deverá, ainda dentro destes prazos, emitir um parecer com previsão de novo prazo, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a

abertura do respectivo chamado.

c Após avaliação deste parecer inicial, o TJCE decidirá sobre a periodicidade da emissão de pareceres ou laudos posteriores, até o fechamento final do atendimento, sem prejuízo da aplicação das penalidades previstas pelo descumprimento dos prazos estabelecidos.

d Em quaisquer casos e quando necessário, a CONTRATADA deverá enviar informações, para o e-mail dos fiscais do contrato, sobre as correções a serem aplicadas ou a própria.

e Caso não haja manifestação da CONTRATADA dentro do prazo definido no **item IX** ou caso os Fiscais do Contrato entendam ser improcedente a justificativa apresentada, será iniciado processo de sugestão de aplicação de penalidades previstas, conforme tabela do **item VII, letra "q" desta cláusula.**

f Após a conclusão do suporte, a CONTRATADA comunicará o fato aos Fiscais do contrato e solicitará autorização para o fechamento do chamado. Caso os mesmos não confirmem a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso os Fiscais do contrato informarão as pendências relativas ao chamado aberto.

g Sempre que houver quebra dos IMR, os fiscais do contrato emitirão notificação à CONTRATADA, ou seu preposto, que terá o prazo de, no máximo, 05 (cinco) dias úteis, contados a partir do recebimento da notificação, para apresentar as justificativas para as falhas verificadas.

h Caso não sejam observados os prazos para atendimento previstos, ou ainda se a justificativa apresentada não for aceita pelos fiscais responsáveis do Contrato, a CONTRATADA estará sujeita a multas/glosas, calculadas sobre o valor descrito mensal do contrato.

i A aplicação das glosas estará restrita ao máximo de 02 (duas) ocorrências (chamados técnicos), podendo ser acumulado os valores de glosas quando alterado a severidade pelo fiscal técnico, durante a vigência do contrato.

j A CONTRATADA ficará sujeita às penalidades previstas, sem prejuízo das Sanções Administrativas constante nesse Termo de Referência.

k O atraso no prazo de solução, de qualquer severidade disposta no **item VII, letra "d",** superior a 25 (vinte e cinco) dias ou após 2 (duas) ocorrências (chamados técnicos) autoriza a Administração aplicar as sanções previstas no **item 11 do ANEXO I deste Edital,** e se for o caso, promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem o inciso I do art. 137 da Lei n.14.133/2021.

l As penalidades previstas neste Termo de Referência não excluem aquelas dispostas na Lei nº 14.133/2021 Art. 162.

X Monitoramento da Execução

a Será efetuado pelos Fiscais Demandantes, Técnicos e Administrativos.

XI Qualidade e Recebimento

a O processo de recebimento do objeto será regido conforme previsto no artigo 140, da Lei nº 14.133/21, e será realizado pelos fiscais do contrato. Acaso precise, pela Comissão de Recebimento de Bens do TJCE.

b Por ocasião do recebimento provisório/definitivo dos produtos/serviços, será assinado documento pertinente, em conformidade com o estabelecido no 140, da Lei nº 14.133/21.

c Forma de Recebimento Provisório – Equipamentos e serviços

1.º) Será considerado o recebimento provisório dos itens objeto desta contratação mediante a entrega destes ao Poder Judiciário Cearense.

2.º) Quando desta entrega, será realizado o recebimento provisório, para efeito de verificação da conformidade dos produtos com as especificações constantes no ANEXO I deste EDITAL.

3.º) Os fiscais do contrato deverão, após a comprovação do perfeito funcionamento do serviço/material, emitir e assinar, em no máximo 5 (cinco) dias úteis, contados do primeiro dia útil posterior à entrega dos serviços/bens, o Termo de Recebimento Provisório.

4.º) Os serviços/bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias úteis, a contar da notificação do Contratante, às suas custas, sem prejuízo da aplicação das penalidades.

5.º) O Contratado deverá informar a SETIN a disponibilidade dos serviços, por meio do endereço eletrônico coordenadoria.seginfo@tjce.jus.br, endereçado aos fiscais do contrato, para que sejam tomadas todas as providências necessárias ao início dos trabalhos.

d Os produtos deverão estar lacrados e não deverão apresentar quaisquer sinais de violação, marcas de quedas, umidades ou quaisquer outros sinais/características que demonstrem avarias, reservado ao Tribunal de Justiça o direito de recusar o recebimento.

1.º) Os fiscais do contrato e a Comissão de Recebimento de Bens Permanentes, caso esta precise atuar, deverão, após comprovado o perfeito funcionamento dos equipamentos e das adequações às especificações técnicas descritas no **Anexo I deste Edital**, emitir e assinar, em no máximo 5 (cinco) dias úteis, contados do primeiro dia útil posterior à entrega dos mesmos, o Termo de Recebimento Provisório, devendo ser entregue à Contratada.

e Forma de recebimento definitivo – Equipamentos e serviços

1.º) No recebimento e aceitação dos equipamentos, serão observadas as especificações contidas **no Anexo I deste Edital** e as disposições contidas no Artigos 140 da Lei 14.133/21 e Lei nº 10.520/02, e suas alterações.

2.º) Após a emissão da ordem de serviço à CONTRATADA, a mesma deverá iniciar, de imediato, a execução dos serviços de instalação e configuração, que deverá ser finalizado dentro do prazo de até 15 (quinze) dias corridos contados da data de emissão da ordem de serviço para a CONTRATADA.

3.º) As especificações serão avaliadas, também, por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e as disponíveis no site do fabricante.

4.º) A solução será recebida definitivamente pelos fiscais do contrato, em até 10 (dez) dias úteis após a instalação / ativação e configuração dos equipamentos / sistemas e entrega da solução em pleno funcionamento e operação, com a devida aprovação dos testes pelos fiscais do contrato da demanda.

5.º) As especificações serão avaliadas, também, por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e as disponíveis no site do fabricante.

6.º) Apresentado o Termo de Recebimento Definitivo e a Nota Fiscal Eletrônica de Venda – devidamente acompanhada dos documentos solicitados no **Anexo I deste Edital**, aos fiscais do contrato e à Comissão de Recebimento de Bens Permanentes, acaso esta precise atuar, devem estes, conjuntamente, atestá-la, encaminhando-a, com o Termo de Recebimento Definitivo, ao Fiscal Administrativo, que após proceder a devida análise no exercício das atribuições regulamentares previstas no § 3º, Art. 24, Seção III da Resolução 468/CNJ, também a atestará, encaminhando-a, posteriormente, ao departamento responsável ao pagamento, com as certidões cabíveis para o feito.

7.º) Se, a qualquer tempo, vier a ser constatado que o equipamento fora fornecido em desacordo com as especificações e, em decorrência desse fato, verificar qualquer tipo de dano ao equipamento no local em que está sendo utilizado, o reparo do equipamento ou, se for o caso, a sua substituição, será de inteira responsabilidade da contratada.

8.º) A Contratada obrigar-se-á a efetuar a troca, às suas expensas, do equipamento que vier a ser recusado, não implicando na aceitação do mesmo o ato de recebimento.

9.º) Ocorrendo qualquer problema de fabricação, a Contratada terá o prazo de 10 (dez) dias úteis para proceder às correções a partir da notificação, adequações ou substituição do (s) produto (s) objeto deste ajuste.

10.º) Caso a correção dos problemas constatados não seja efetuada no período de até 10 (dez) dias úteis, contados a partir da data da primeira notificação, a Contratada deverá trocar os equipamentos em até 48 horas e em definitivo, sem ônus para o TJCE;

11.º) Caso os equipamentos contratados não atendam ao especificado ou apresentem defeitos, serão considerados não entregues e a contagem do prazo de entrega não será interrompida devido à rejeição dos mesmos. Neste caso, a Contratada arcará com o (s) ônus decorrente (s) desse atraso, passível de penalidade, conforme disposto no item **11** do **Anexo I deste Edital.**

12.º) O aceite e o posterior pagamento dos equipamentos/serviços não eximem a licitante vencedora das responsabilidades pela correção de todos os defeitos, falhas e quaisquer outras irregularidades.

f Forma de recebimento definitivo Objeto – Suporte Técnico

1.º) A garantia da solução será de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo, e engloba os cabos e módulos objetos do presente no Termo de Referência, incluindo assistência corretiva, compreendendo a substituição de peças, componentes que apresentem defeito durante este período, sem qualquer ônus adicional para o TJCE, obrigando-se a Contratada a manter os materiais permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, assim como o pleno funcionamento dos software contratados.

2.º) Todos os custos referentes à coleta, transportes e devolução dos materiais, no período de garantia, são de responsabilidade da Contratada.

3.º) A garantia técnica compreende todas as funcionalidades dos materiais adquiridos, tanto as descritas neste Termo de Referência, quanto as contempladas nos manuais e demais documentos técnicos.

i. Será efetuada pela Contratada, sem ônus para o Contratante, a troca de todas e quaisquer partes, peças e equipamentos que se revelarem defeituosos, independentemente de causa ou do tipo de defeito.

ii. Todas as peças e componentes substituídos deverão ser originais ou certificados pelo fabricante e sempre "novos e de primeiro uso", não podendo ser recondicionados, com apresentação de documentos para tanto.

iii. O serviço de garantia/suporte prestado deverá ser realizado no idioma português (Brasil).

iv. Caso o equipamento, identificado pelo seu número de série, apresente o mesmo defeito recorrente após o segundo conserto, a Contratada deverá substituí-lo por outro idêntico ou superior, sem qualquer ônus para o TJCE.

v. Os parâmetros para abertura de chamado para Assistência Técnica estão contidos no **item VII.**

g Forma de avaliação da qualidade dos bens e/ou serviços entregues

1.º) Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, o TJCE, através dos fiscais do contrato, realizará, anualmente, a Avaliação de Desempenho, o que permitirá a adoção de eventuais ajustes no modelo de atendimento, conforme critérios abaixo, podendo ser criados outros que se fizerem necessários.

2.º) Comunicação: Avaliação qualitativa da comunicação do Contratado, como clareza na informação, formas de solicitações e questionamentos ao TJCE, educação e nível de formalidade no atendimento e tempo de resposta às solicitações.

3.º) Confiabilidade: Prestação correta (isenta de falhas e erros) do serviço/atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas.

4.º) Organização: Demonstração de planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

5.º) Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos conceitos abaixo:

6.º) Péssimo (de 0 a 4,9) / Regular (de 5 a 7,4) / Bom (de 7,5 a 8,9) / Ótimo (de 9 a 10).

7.º) Anualmente, a empresa contratada será informada do conceito médio obtido no período e registrado nos autos do contrato, resultado este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

CLÁUSULA QUINTA – DO PREÇO, PRAZO E CONDIÇÕES DE PAGAMENTO

A CONTRATANTE pagará à CONTRATADA, pelos serviços prestados, o valor global anual de R$_____ (_____), referente aos serviços descritos no Anexo____ deste Termo de Contrato.

1 A CONTRATADA deverá observar, quanto aos prazos, custo e forma de pagamento, as seguintes diretrizes:

I Os pagamentos serão realizados através de depósito bancário, preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento mensal e definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade com as medições realizadas, validado previamente pela CONTRATANTE atestada pelo setor competente deste Tribunal de Justiça, via emissão do Termo de Recebimento Definitivo, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

II O prazo para pagamento de faturas ou notas fiscais serão suspensos durante o período de indisponibilidade do sistema de pagamento do Estado do Ceará ao final de cada exercício financeiro, aproximadamente entre 20 de dezembro e 31 de janeiro do ano subsequente, cujos pagamentos serão realizados até o final da primeira quinzena do mês de fevereiro.

III O Tribunal de Justiça reserva-se ao direito de recusar o pagamento, no ato do atesto, caso o objeto

não esteja em conformidade com as condições deste instrumento.

IV Nenhum pagamento será efetuado à empresa antes regularizada as sanções que por ventura lhe tenham sido aplicadas.

V Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a CONTRATADA fazer a substituição desta(s) NF(s) / Fatura(s).

VI Nas notas fiscais referentes aos serviços objeto do contrato, deverão estar descriminados os valores dos tributos: impostos sobre serviços – ISS, PIS/PASEP, COFINS, FUST, FUNTTEL;

VII Os serviços de suporte e manutenção serão faturados mensalmente após a solicitação de pagamento por parte da CONTRATADA, sendo o pagamento condicionado ao aceite do Relatório de Instrumento de Medição de Resultados, item 5.5.4 do Anexo I deste Edital, por parte da CONTRATANTE.

a O valor do pagamento mensal estará diretamente vinculado ao índice alcançado para os indicadores estabelecidos, sendo pago conforme resultado obtido e decrementado (cumulativamente) quando não forem atingidas as metas exigidas.

b Caso a CONTRATADA não cumpra com os seus compromissos, de qualidade e desempenho, terá a sua fatura reduzida conforme estabelecido no item 5.7.16 do Anexo I deste Edital.

c Os redutores deverão ser levantados pela Contratada, anexados à solicitação de pagamento, sendo validados pelo TJCE. Os redutores serão aplicados sobre o faturamento mensal na ocorrência dos fatos geradores, independentemente da abertura de processo administrativo.

VIII Constatada a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

IX Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, 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.

X Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

XI Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação

XII Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.

XIII Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) ser emitida(s) em nome do Tribunal de Justiça do Estado do Ceará, CNPJ N.º 09.444.530/0001-01 e estar em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

XIV O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual.

XV Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

XVI Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

XVII A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

2 Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos Moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365} \qquad I = \frac{6/100}{365} \qquad I = 0,00016438$$

no qual i = taxa percentual anual no valor de 6% (seis por cento).

CLÁUSULA SEXTA – DO REAJUSTE E DOS RECURSOS ORÇAMENTÁRIOS

A CONTRATANTE atenderá às prescrições para reajustamento do contrato nos termos definidos nesta cláusula.

1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data de apresentação da proposta.
2 Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do **Índice de Custo da Tecnologia da Informação (ICTI) - Ipea**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
3 O processo referente ao pedido de reajuste supra, deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.
4 Os recursos financeiros serão decorrentes do financiamento contraído junto ao Banco Interamericano de Desenvolvimento – BID, no âmbito do Programa de Modernização do Poder Judiciário do Estado do Ceará (PROMOJUD), tendo como fonte os Recursos de Operações de Crédito, nas seguintes dotações orçamentárias:

04200021.02.126.192.11470.15.449052.1.759.1200070.1.20 (00475)
04200021.02.126.192.11470.15.449052.2.759.1200070.1.20 (-)
04200021.02.126.192.20511.15.339040.1.759.1200070.1.20 (08290)
04200021.02.126.192.20511.15.339040.2.759.1200070.1.20 (-)
04200021.02.126.192.20512.15.339040.1.759.1200070.1.20 (23584)
04200021.02.126.192.20512.15.339040.2.759.1200070.1.20 (-)

5 Nenhuma contratação será efetuada sem a prévia indicação da disponibilidade orçamentária.
6 Foi emitida pelo TJCE a Nota de Empenho n. ....., de ...../...../....., no valor de R$ ___._____,____ (.....), à conta da Dotação Orçamentária especificada nesta Cláusula, para fazer face às despesas inerentes a este Termo de Contrato.

CLÁUSULA SÉTIMA – DOS ELEMENTOS PARA GESTÃO DO CONTRATO

Os elementos para a gestão do contrato serão processados da seguinte forma:

1 Forma de Acompanhamento do Contrato:

ID	Evento	Forma de Acompanhamento
1	Da entrega da solução	O recebimento do objeto deverá ocorrer conforme definido no item 5 e seus subitens do **ANEXO I deste Edital.**
2	Durante a vigência do Contrato	Será verificado o cumprimento do prazo de solução dos chamados, conforme descrito do **ANEXO I deste Edital.**

2 Prazos e Condições

I Os prazos são detalhados na seguinte Tabela:

N.º	Etapa	Quando	Responsável
1	Reunião de alinhamento	Em até 5 (cinco) dias úteis após a data de assinatura do contrato.	CONTRATANTE e CONTRATADA
2	Entrega do hardware	Em até 30 (trinta) dias corridos após a data de emissão da ordem de fornecimento pela Contratante.	CONTRATADA
3	Instalação, configuração e testes da solução	Em até 5 (cinco) dias corridos contados da data de emissão da ordem de serviço pela Contratada.	CONTRATADA
4	Conclusão da Instalação, configuração e testes da solução	Em até 15 (quinze) dias úteis contados a partir da data de emissão da ordem de serviço pela Contratada.	CONTRATADA
5	Operação assistida	Após as atividades de instalação, configuração e migração tecnológica, deve ser iniciada a operação assistida para os itens 1 a 3 que consta na tabela do item 1.2, com duração de 20 dias úteis, podendo ser prolongada no caso de percepção por parte do TJCE de pendências impeditivas à emissão de recebimento definitivo dos serviços até que sejam sanadas para o atendimento dos requisitos técnicos.	CONTRATADA
6	Treinamento	Está condicionada à solicitação prévia, via emissão de ordem de serviço por parte da Contratante, em data a ser previamente acordada com o TJCE.	CONTRATADA
7	Documentação	Após a emissão do Termo de Recebimento Definitivo, a contratada deverá, em até 5 dias úteis, entregar ao Tribunal documentação de as-built de cada serviço.	CONTRATADA
8	Início do período de validade/vigência dos licenciamentos. Início do período de prestação de serviço de suporte técnico e garantia da solução.	60 (sessenta) meses após a emissão do Termo de Recebimento Definitivo.	CONTRATADA
9	Regime para atendimento da garantia on-site	NBD – Next Business Day (próximo dia útil) em atendimento no regime 24x7 (24 horas por dia, 7 dias na semana).	CONTRATADA

3 Estimativa do Volume de Bens/Serviço:

ID	Bem	Estimativa	Forma de Estimativa
1	Firewall – Hardware	Duas Unidades	A quantidade de firewalls e todos os seus requisitos técnicos foram definidos após análise dos requisitos de negócio e técnicos da área demandante. Para a definição dos quantitativos, foram consideradas a atual quantidade de dois equipamentos utilizados na solução de segurança. O alinhamento entre os requisitos do objeto desta contratação e os requisitos da área de negócio estão detalhados nos estudos técnicos preliminares.
2	Software Gerenciamento centralizado e relatoria	Uma unidade	Para a definição dos quantitativos, foram consideradas a atual quantidade de equipamentos utilizados na solução de segurança.
3	Solução para acesso remoto seguro e a aplicações privadas	Licença para 2000 usuários	Para a definição dos quantitativos, foram consideradas a atual quantidade de usuários utilizando a solução atual de segurança.
4	Serviço de instalação	Uma unidade	Para a definição dos quantitativos, foram consideradas a quantidade de serviço necessário para instalação do novo equipamento a ser adquirido.
5	Serviço de suporte técnico e monitoramento 24x7	Serviço para 60 meses	Para a definição dos quantitativos, foram consideradas a quantidade de meses da garantia do novo equipamento a ser adquirido.
6	Treinamento	1 unidade para 8 pessoas	Para a definição dos quantitativos, foram consideradas a quantidade de servidores da SETIN com demandas da área de segurança da informação

4 Propriedade, sigilo e restrições:

I A CONTRATADA cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do Art. 93, da LEI Nº 14.133, DE 1º DE ABRIL DE 2021, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência do objeto contratado, entendendo-se por resultados quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros.
II Toda a documentação produzida pela CONTRATADA referente à implantação dos equipamentos e documentos exigidos no termo de referência passam a ser propriedade de forma perpétua do TJCE, não precisando este Tribunal de autorização da CONTRATADA para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

III Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a CONTRATADA, zelar por si, por seus sócios, empregados e subcontratados (em outros contratos) pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso.
IV A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a CONTRATADA, previstas no CONTRATO e na legislação pertinente.
V Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados que, a qualquer título, venham a integrar a equipe executante do Objeto, a assinatura do **ANEXO I - TERMO DE CIÊNCIA**, bem como a assinatura do **ANEXO II - TERMO DE COMPROMISSO**, onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.
VI A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte, mediante assinatura do Termo de Confidencialidade constante no ANEXO I deste EDITAL.

5 Mecanismos formais de comunicação:

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Emissão da Ordem de serviço/fornecimento	Contratante	Contratada	Ordem de serviço/fornecimento	Quando demandado pela SETIN.
Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
Abertura de chamados de garantia. Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado;	Contratante	Contratada	E-mail, telefone e site na internet	Quando demandado pela SETIN.
Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, e-mail, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet,	Quando necessário

			PDF (*Portable Document Format*): documento em formato portável.	

CLÁUSULA OITAVA – DA GARANTIA DOS SERVIÇOS

A especificação da garantia do serviço deverá observar o art. 40, §1º, inciso III, da Lei nº 14.133, de 2021.

1 A garantia contratual dos serviços, complementar à garantia legal, deve atender as especificações técnicas dos itens 5.11.6.1, 4, 13 e 15 do **ANEXO I deste Edital,** pelo prazo mínimo contratual de 60 (sessenta) meses, contado a partir do primeiro dia útil subsequente à data do TRD.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

A Adjudicatária deverá oferecer, a título de garantia do contrato, a partir da data de homologação, e conforme o Art. 98, da Lei nº 14.133/2021 e suas alterações, 5% (cinco por cento) do valor anual do contrato, devidamente atualizado.

1 Será concedido prazo mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para a prestação da garantia pelo contratado quando optar pela modalidade seguro-garantia. As demais modalidades deverão ser apresentadas em até 5 (cinco) dias, a contar da assinatura do Termo de Homologação.
2 A garantia prestada será restituída e/ou liberada **90 (noventa) dias** após o término da vigência contratual, desde que cumpridas integralmente todas as obrigações contratuais; quando em dinheiro, será atualizada monetariamente, conforme dispõe o art. 100, da Lei nº. 14.133/2021.
3 Poderá o contratado optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, nos termos do art. 96, § 1º, da Lei 14.133/2021.
4 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, devendo acompanhar as modificações referentes ao valor e à vigência desta mediante a complementação da caução ou emissão do respectivo endosso pela seguradora ou instituição financeira bancária fiadora.
5 Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.
6 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

I Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

II Prejuízos diretos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

III Multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

IV Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

7 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.
8 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

I A não complementação ou renovação, tempestiva, da garantia do contrato ensejará a suspensão de pagamentos até a regularização do respectivo documento, independentemente da aplicação das sanções contratuais.

II A inobservância do prazo fixado para apresentação, complementação ou renovação da garantia acarretará a aplicação das sanções previstas neste Termo de Contrato.

9 O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

10 O emitente da garantia ofertada pela contratada deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

11 Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

12 Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato;

13 A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

14 A garantia somente será liberada ante a comprovação de que o contratado pagou todas as verbas rescisórias decorrentes da contratação, sendo que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia deverá ser utilizada para o pagamento dessas verbas trabalhistas, incluindo suas repercussões previdenciárias e relativas ao FGTS, observada a legislação que rege a matéria;

15 Também poderá haver liberação da garantia se a empresa comprovar que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho;

16 Por ocasião do encerramento da prestação dos serviços contratados, a Administração Contratante poderá utilizar o valor da garantia prestada para o pagamento direto aos trabalhadores vinculados ao contrato no caso da não comprovação: (1) do pagamento das respectivas verbas rescisórias ou (2) da realocação dos trabalhadores em outra atividade de prestação de serviços.

17 O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

18 A CONTRATADA autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no Contrato.

CLÁUSULA DEZ – DAS SANÇÕES ADMINISTRATIVAS

Quanto às sanções administrativas, deve-se observar o disposto nesta cláusula.

1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a contratado que:

I deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pela Administração, em sede de diligência.

II salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

a não enviar a proposta ajustada após a negociação;

b recusar-se a enviar o detalhamento da proposta quando exigível;

c pedir para ser desclassificado quando encerrada a etapa competitiva;

d deixar de apresentar amostra, quando exigível.

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

IV recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

V apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

VI fraudar a licitação.

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

a agir em conluio ou em desconformidade com a lei;

b induzir deliberadamente a erro no julgamento;

c apresentar amostra falsificada ou deteriorada;
d praticar atos ilícitos com vistas a frustrar os objetivos da contratação;
e praticar ato lesivo previsto no art. 5° da Lei 12.846/2013.

VIII A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido no instrumento convocatório, descrita no item I, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação. A exigência da garantia obedecerá ao disposto no art. 58 da Lei nº 14.133/2021.

IX Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar a contratada as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

a advertência;
b multa;
c impedimento de licitar e contratar; e
d declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

X Na aplicação das sanções serão considerados:

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

XI A sanção de multa calculada na forma do edital ou do contrato, não será inferior a 0,5% (cinco décimos por cento), nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.

XII A LICITANTE VENCEDORA, uma vez contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o complementem, às sanções e penalidades administrativas, inclusive multas.

XIII Caso a Contratada se torne inadimplente na execução dos serviços, a Contratante poderá, sem prejuízo de outras medidas, a título de multa, o equivalente a 0,5% (cinco décimos por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, para a conclusão da demanda, nos termos e condições dispostas no Termo de Referência – ANEXO I deste Edital, sem prejuízo das sanções legais e responsabilidades civil e criminal.

XIV Caso a Contratada se torne inadimplente na execução dos serviços, a Contratante poderá, sem prejuízo de outras medidas, a título de multa, o equivalente a 0,5% (cinco décimos por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, para a conclusão da demanda, nos termos e condições dispostas no Termo de Referência, sem prejuízo das sanções legais e responsabilidades civil e criminal.

XV A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

XVI Os percentuais de multas aplicadas incidirão sempre sobre do valor global do termo de contrato licitado ou celebrado ou instrumento equivalente.

XVII As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

XVIII Na aplicação da sanção será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

XIX A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos **itens I,II e III**, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

XX Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos **itens IV, V, VI e VII**, bem como pelas infrações administrativas previstas nos **itens I,II e III** que justifiquem a imposição de penalidade mais grave

que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

XXI A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

XXII Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual 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, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

XXIII Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

XXIV O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

XXV A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

XXVI Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

XXVII As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.

XXVIII Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

XXIX Independente de outras sanções legais e das cabíveis penais, pela inexecução total ou parcial da contratação, a administração poderá, garantida a prévia defesa, aplicar à empresa licitante, segundo a extensão da falta cometida, as seguintes penalidades, previstas no art. 156 da Lei n. 14.133/23:

a Aplicação de multa administrativa, além das Glosas previstas no item 5.7 do ANEXO I deste Edital.

b Na ordem de 20% (vinte por cento) sobre o valor total da contratação, nas hipóteses de inexecução total ou violação do sigilo.

c Na ordem de 0,5% do valor total da contratação, ao dia de suspensão ou interrupção, total ou parcial, salvo motivo de força maior, caso fortuito ou autorização do fiscal, dos serviços de instalação, configuração, suporte técnico ao total de 10%, moratório.

d Na ordem de 1% sobre o valor da Nota Fiscal em questão, ao dia pelo não cumprimento do conteúdo disposto nos itens **5.3.6** e **5.11.5.11** do Anexo I deste Edital, limitado ao total de 20%.

e Caso os limites do **item XXVIII, letras "c" e "d"** sejam excedidos, configura-se então casos de inexecução contratual.

CLÁUSULA ONZE – DA EXTINÇÃO CONTRATUAL

O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

1 Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

2 Quando a não conclusão do contrato referida no parágrafo anterior decorrer de culpa da CONTRATADA:

I Ficará ela constituída em mora, sendo-lhe aplicáveis as respectivas sanções administrativas;

II Poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

3 O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

I Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

II A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

III Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

4 A extinção do contrato não configura óbice para o reconhecimento do 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).

5 O contrato poderá ser extinto caso se constate que o contratado mantém 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 (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DOZE – DA SUBCONTRATAÇÃO

Não será permitida a subcontratação total ou parcial do objeto deste Termo de Contrato.

1 Não será admissível a fusão, cisão ou incorporação da CONTRATADA.

CLÁUSULA TREZE – DOS CRITÉRIOS AMBIENTAIS

A CONTRATADA deverá providenciar o recolhimento e o adequado descarte de produto(s) e material(is) inservível(is) originário(s) da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA n° 01, de 18/03/2010, da Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA n° 416, de 30/09/2009, e legislação correlata.

1 A CONTRATADA deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 11º da Lei n.º 14.133/21.

2 Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

3 Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4 Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva ROHS (*restriction of certain hazardous substances*), tais como mercúrio (hg), chumbo (pb), cromo hexavalente (cr(vi)), cádmio (cd), bifenil-polibromados (pbbs), éteres difenil-polibromados (pbdes).

5 Os serviços prestados e os bens fornecidos pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

CLÁUSULA QUATORZE – DO PRAZO DE VIGÊNCIA DO CONTRATO

O prazo de vigência deste termo de contrato será de 60 (sessenta) meses, contados da assinatura do CONTRATO, podendo ser prorrogado até limite permitido pela Lei 14.133/21, e conforme a conveniência estabelecida entre CONTRATADA e CONTRATANTE.

CLÁUSULA QUINZE – DO GESTOR DO CONTRATO E DO ORDENADOR DE DESPESAS

O órgão responsável pela contratação é o Tribunal de Justiça do Estado do Ceará.

1 O Gestor do Contrato será a(o) Secretária(o) de Tecnologia da Informação do TJCE ou profissional por ela(e) indicado devidamente oficializado por meio de publicação no Diário da Justiça Eletrônico.
2 Os Ordenadores de Despesas serão o(a) Desembargador(a) Presidente do Tribunal de Justiça do Estado do Ceará conjuntamente com a(o) Secretária(o) de Tecnologia da Informação do TJCE, conforme Portaria n. 310/2023, disponibilizada no DJe de 09 de fevereiro de 2023, que dispõe sobre a delegação de competências administrativas no âmbito do Poder Judiciário do Estado do Ceará.

CLÁUSULA DEZESSEIS – DAS ALTERAÇÕES CONTRATUAIS

As alterações ao presente contrato poderão ser necessárias se ocorrerem quaisquer das situações previstas no artigo 124 da Lei Federal nº 14.133/21.

PARÁGRAFO ÚNICO – A CONTRATADA deverá aceitar, nas mesmas condições propostas, os acréscimos ou as supressões que se fizerem necessária, até o limite de 25% do valor inicial do contrato, nos termos do artigo 125 da Lei n° 14.133/21.

CLÁUSULA DEZESSETE – DA LEGISLAÇÃO APLICÁVEL

Este termo de contrato rege-se pela Lei n° 14.133/21 e suas alterações, pela legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

CLÁUSULA DEZOITO – DO FORO

Fica eleito o foro de Fortaleza (CE), para dirimir quaisquer dúvidas oriundas do presente Termo de Contrato, caso não possam ser resolvidos por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

PARÁGRAFO ÚNICO – Firmam o presente em 2 (duas) vias de igual teor e forma, por estarem justos e acertados, na presença da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça Eletrônico (DJe).

Fortaleza, ____ de _____ de 20___.

_____
CONTRATANTE

_____
CONTRATADO(A)

Testemunhas:

1._____
RG:
CPF:

2._____
RG:
CPF:

ANEXO I DO CONTRATO

ESPECIFICAÇÃO TÉCNICA

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. DESCRIÇÃO DOS SERVIÇOS E QUANTITATIVO

Id	Bem/Serviço	Model/Part Num-ber	Qtd.
1	PA-5410 with redundant AC power supplies 60 meses – Palo Alto Networks	PAN-PA-5410-AC	2
2	PA-5410 –60 meses– Palo Alto Networks Core Security Subscription Bundle: Advanced Threat Prevention Advanced URL Filtering Advanced Wildfire DNS Security SD-WAN)	PAN-PA-5410-BND-CORESEC-5YR	2
3	GlobalProtect subscription, for device in an HA pair, PA-5410 -60 meses – Palo Alto Networks	PAN-PA-5410-GP-5YR	2
4	Zero Trust Network Access (ZTNA) com capacidade para suportar 400 usuários. 60 meses – Palo Alto Networks	PAN-PRISMA-ACCESS-MU-LCL-ENTERPRISE + PAN-PRISMA-ACCESS-PREM-SUCCESS +PAN-CDL-1TB	1
5	Panorama management software, 25 devices 60 meses – Palo Alto Networks	PAN-PRA-25	1
6	Premium support prepaid, Panorama 25 devices 60 meses – Palo Alto Networks	PAN-SVC-PREM-PRA-25-5YR	1
7	Premium support term, PA-5410 60 meses – Palo Alto Networks	PAN-SVC-PREM-5410-5YR	2
8	Implantação da solução de Firewall	---	1
9	Treinamento para até 08 (oito) pessoas. Carga horária de 40h	---	1
10	Serviço de instalação e repasse de conhecimento para solução de zero trust network access (ztna)	---	1
11	Serviço de Suporte Técnico e monitoramento 24x7 para next generation firewall em alta disponibilidade - prazo do contrato: 60 meses	---	1

2. ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

2.1. NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.1.1. CARACTERÍSTICAS GERAIS

2.1.1.1. A solução deve incluir um par de equipamentos (appliances) Next Generation Firewall em alta disponibilidade, bem como uma solução

de gerenciamento centralizado e relatoria, todos fornecidos pelo mesmo fabricante. Cada par de equipamentos de alta disponibilidade deve ser projetado especificamente para a função de Next Generation Firewall, com hardware e software também provenientes do mesmo fabricante.

2.1.1.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, de forma integrada e simultânea, as funcionalidades de firewall, identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware Protection, Anti-Spyware), administração de largura de banda de serviço de Internet (QoS – Quality of Service), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL;

2.1.1.3. O equipamento e seus componentes deverão ser novos, sem uso, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

2.1.1.4. Não será aceito equipamento em modo End of Life e End of Support.

2.1.1.5. Não serão aceitas soluções baseadas em PCs de uso geral.

2.1.1.6. A solução deve suportar a configuraçao de alta disponibilidade, podendo ser configurado ativo/passivo ou ativo/ativo, com consideração para licenciamento adicional, se necessário.

2.1.1.7. Todos os componentes necessários para o pleno funcionamento da solução devem ser fornecidos.

2.1.1.8. Todas as funcionalidades que dependam de licenciamento devem ser entregues licenciadas para 60 meses.

2.1.2. CARACTERÍSTICAS FÍSICAS MÍNIMAS

2.1.2.1. Deve possuir throughput de, no mínimo, 26 Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

2.1.2.2. Cada equipamento (appliance) que compõe a solução de alta disponibilidade deve suportar, e estar licenciado para a criação de pelo menos 10 (dez) sistemas virtuais, independentes entre si.

2.1.2.3. Deve suportar, no mínimo, 3.500.000 conexões simultâneas;

2.1.2.4. Deve suportar, no mínimo, 250.000 novas conexões por segundo;

2.1.2.5. Deve suportar, no mínimo, 7 (sete) Gbps de throughput de Inspeção SSL;

2.1.2.6. Deve possuir, no mínimo, 8 (oito) interfaces físicas de rede de 1/10 Gbps do tipo RJ-45;

2.1.2.7. Deve possuir, no mínimo, 12 (doze) interfaces físicas de rede de 1/10 Gbps do tipo SFP/SFP+.

2.1.2.8. Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 40/100 Gbps do tipo QSFP+/QSFP28.

2.1.2.9. Deve possuir, no mínimo, 2 (duas) interface física dedicada para

o sincronismo de estados da solução de alta disponibilidade;

2.1.2.10. Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

2.1.2.11. Deve possuir, no mínimo, 1 (uma) interface dedicada para gerenciamento;

2.1.2.12. Deve possuir armazenamento interno redundante de, no mínimo, 480 GB;

2.1.2.13. Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 e 240 VAC e devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento; deverá vir acompanhado de cabo de alimentação.

2.1.2.14. O equipamento deve ser fornecido com as portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para uso, sem custos adicionais. Todas as interfaces solicitadas nos appliances devem estar licenciadas e prontas para uso imediato, incluindo os transceivers/transceptores considerando o padrão Short Range (SR).

2.1.3. FUNCIONALIDADE DE FIREWALL

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

2.1.3.2. Suporte aos protocolos IPv4 e IPv6.

2.1.3.3. Suporte a no mínimo 512 VLANs no padrão 802.1q

2.1.3.4. Agregação de links 802.3ad e LACP;

2.1.3.5. Policy based routing ou policy-based forwarding;

2.1.3.6. Roteamento multicast (PIM-SM);

2.1.3.7. Deve suportar os protocolos IGMP v2, IGMP v3;

2.1.3.8. Deve suportar os protocolos DHCP e DHCPv6;

2.1.3.9. Deve suportar o protocolo NTP;

2.1.3.10. Jumbo Frames;

2.1.3.11. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

2.1.3.12. Suportar sub-interfaces ethernet logicas;

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

2.1.3.14. Deve implementar Network Prefix Translation (NPTv6) ou NAT66;

2.1.3.15. Enviar log para sistemas de monitoração externos;

2.1.3.16. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

2.1.3.17. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

2.1.3.18. Proteção contra anti-spoofing;

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

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

2.1.3.21. Suportar a OSPF graceful restart;

2.1.3.22. Deve suportar o protocolo MP-BGP (Multiprotocol BGP)

permitindo que o firewall possa anunciar rotas para IPv4 e IPv6;

2.1.3.23. 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);

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

2.1.3.25. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

2.1.3.26. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

2.1.3.27. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

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

2.1.3.29. A configuração em alta disponibilidade deve sincronizar:

2.1.3.29.1. Sessões;

2.1.3.29.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

2.1.3.29.3. Certificados de-criptografados;

2.1.3.29.4. Associações de Segurança das VPNs;

2.1.3.29.5. Tabelas FIB;

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

2.1.4. CONTROLE POR POLÍTICA DE FIREWALL

2.1.4.1. Deverá suportar controles por zona de segurança;

2.1.4.2. Controles de políticas por porta e protocolo;

2.1.4.3. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

2.1.4.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

2.1.4.5. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

2.1.4.6. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

2.1.4.7. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

2.1.4.8. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);

2.1.4.9. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);

2.1.4.10. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

2.1.4.11. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com HTTP/2, TLS 1.2 e 1.3;

2.1.4.12. Controle de inspeção e de-criptografia de SSH por política;

2.1.4.13. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

2.1.4.14. Bloqueios de arquivos por extensão;

2.1.4.15. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);

2.1.4.16. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;

2.1.4.17. Suporte a objetos e regras IPV6;

2.1.4.18. Suporte a objetos e regras multicast;

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

2.1.5. CONTROLE DE APLICAÇÕES

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

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

2.1.5.3. Reconhecer pelo menos 3000 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;

2.1.5.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

2.1.5.5. 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;

2.1.5.6. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

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

2.1.5.8. Atualizar a base de assinaturas de aplicações automaticamente;

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

2.1.5.10. 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;

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

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

2.1.5.13. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

2.1.5.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações customizadas;

2.1.5.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

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

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

2.1.5.18. Deve permitir criar filtro na tabela de regras de segurança para exibir somente:

2.1.5.19. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;

2.1.5.20. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra;

2.1.5.21. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;

2.1.6. IDENTIFICAÇÃO DE USUÁRIOS

2.1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

2.1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.1.6.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

2.1.6.4. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

2.1.6.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x ou soluções NAC via syslog, para a identificação de endereços IP e usuários;

2.1.6.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

2.1.6.7. Suporte a autenticação Kerberos;

2.1.6.8. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

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

2.1.6.10. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;

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

2.1.7. QOS

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

2.1.7.2. Suportar a criação de políticas de QoS por:

2.1.7.3. Endereço de origem

2.1.7.4. Endereço de destino

2.1.7.5. Por usuário e grupo do LDAP/AD.

2.1.7.6. Por aplicações;

2.1.7.7. Por porta;

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

2.1.7.9. Banda Garantida

2.1.7.10. Banda Máxima

2.1.7.11. Fila de Prioridade.

2.1.7.12. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

2.1.7.13. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

2.1.7.14. Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

2.1.7.15. Deve suportar QOS (traffic-shapping), em interface agregadas;

2.1.7.16. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

2.1.8. VPN

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

2.1.8.2. Suportar IPSec VPN;

2.1.8.3. Suportar SSL VPN;

2.1.8.4. A VPN IPSEc deve suportar:

2.1.8.5. 3DES;

2.1.8.6. Autenticação MD5 e SHA-1;

2.1.8.7. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

2.1.8.8. Algoritmo Internet Key Exchange (IKEv1 e v2);

2.1.8.9. AES 128 e 256 (Advanced Encryption Standard);

2.1.8.10. Autenticação via certificado IKE PKI;

2.1.8.11. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

2.1.8.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

2.1.8.13. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

2.1.8.14. Deve suportar a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

2.1.8.15. Deve suportar a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

2.1.8.16. O cliente de VPN SSL deve ser capaz de ser insalado e estar devidamente licenciado para criar perfis customizados de conformidade no mínimo os seguintes sistemas operacionais:

2.1.8.16.1. Windows;

2.1.8.16.2. MacOS

2.1.8.16.3. Linux;

2.1.8.16.4. Android

2.1.8.16.5. Apple iOS.

2.1.8.17. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

2.1.8.18. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto:

2.1.8.18.1. Sistema operacional e patches instalados;

2.1.8.18.2. Antivírus e versão instalada;

2.1.8.18.3. Firewall no host;

2.1.8.18.4. Criptografia do disco;

2.1.8.18.5. Agente de DLP instalado;

2.1.8.18.6. Backup de disco;

2.1.8.18.7. Chaves de registros;

2.1.8.18.8. Processos ativos.

2.1.8.19. Deve permitir a quarentena automática e manual de dispositivos caso encontre algum comprometimento malicioso no tráfego inspecionado.

2.1.8.20. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções:

2.1.8.20.1. sistema operacional e patches instalados;

2.1.8.20.2. Antivírus e versão instalada;

2.1.8.20.3. Firewall no host;

2.1.8.20.4. Criptografia do disco;

2.1.8.20.5. Agente de DLP instalado backup de disco;

2.1.8.20.6. Chaves de registros

2.1.8.20.7. Processos ativos;

2.1.9. PREVENÇÃO DE AMEAÇAS

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

2.1.9.2. Deve ter a capacidade de bloquear ameaças desconhecidas em tempo real;

2.1.9.3. 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;

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

2.1.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

2.1.9.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

2.1.9.7. Deve permitir o bloqueio de vulnerabilidades.

2.1.9.8. Deve permitir o bloqueio de exploits conhecidos.

2.1.9.9. Deve incluir proteção contra ataques de negação de serviços.

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

2.1.9.11. Análise de padrões de estado de conexões;

2.1.9.12. Análise de decodificação de protocolo;

2.1.9.13. Análise para detecção de anomalias de protocolo;

2.1.9.14. Análise heurística;

2.1.9.15. IP Defragmentation;

2.1.9.16. Remontagem de pacotes de TCP;

2.1.9.17. Bloqueio de pacotes malformados.

2.1.9.18. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

2.1.9.19. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

2.1.9.20. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

2.1.9.21. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.1.9.22. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

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

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

2.1.9.25. Identificar e bloquear comunicação com botnets;

2.1.9.26. Deve ser capaz de analisar em tempo real através de mecanismos baseados em Machine Learning o tráfego de ameaças avançadas de C2 (comando e controle) e spyware para proteção de ameaças de dia zero.

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

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

2.1.9.27.2. Deve suportar a captura de pacotes (PCAP), por assinatura de Malware e aplicação;

2.1.9.27.3. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

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

2.1.9.27.5. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

2.1.9.27.6. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos;

2.1.9.27.7. Rastreamento de vírus em pdf;

2.1.9.27.8. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);

2.1.10. FILTRO WEB

2.1.10.1. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

2.1.10.2. Deve suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

2.1.10.3. Deve possuir pelo menos 60 categorias de URLs;

2.1.10.4. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.1.10.5. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade;

2.1.10.6. Deve suportar a capacidade de criação de políticas baseadas no controle por URL ou categoria de URL;

2.1.10.7. Deve suportar a criação categorias de URLs customizadas;

2.1.10.8. Deve possuir a função de exclusão de URLs do bloqueio;

2.1.10.9. Deve permitir a customização de página de bloqueio;

2.1.10.10. Deve 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);

2.1.10.11. Deve permitir controlar o envio de credenciais corporativas somente para categorias de URLs permitidas;

2.1.10.12. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

2.1.10.13. Deve prover análise em tempo real do conteúdo web e dessa forma permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução;

2.1.10.14. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

2.1.11. ANÁLISE DE MALWARES MODERNOS

2.1.11.1. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

2.1.11.2. Deve ser capaz de enviar para análise, arquivos tipo Executáveis, DLLs, Arquivos de Código e MSI;

2.1.11.3. Suportar a análise de arquivos maliciosos em ambiente

controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Android, Linux.

2.1.11.4. A solução deve possuir a capacidade de extrair e analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

2.1.11.5. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

2.1.11.6. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

2.1.11.7. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

2.1.11.8. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

2.1.11.9. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

2.1.11.10. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

2.1.11.11. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

2.1.11.12. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.1.11.13. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

2.1.11.14. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

2.1.11.15. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

2.1.11.16. A solução deve analisar os arquivos do tipo malware em bare metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executem esta função.

2.1.11.17. Deve previnir contra ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.

2.1.11.18. Deve ser capaz de aplicar de forma complementar às assinaturas de antivirus a inspeção inline através de Machine learning em tempo real arquivos tipo PE (portable executable), ELF (executable and linked format) e Arquivos Microsoft Office, bem como, scripts PowerShell e shell script em tempo real para malwares desconhecidos;

2.1.12. PROTEÇÃO DNS

2.1.12.1. Deve possuir a função resolução de endereços via DNS, para que

conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

2.1.12.2. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.1.12.2.1. Domínio suspeito identificado;

2.1.12.2.2. ID de assinatura de detecção;

2.1.12.2.3. Usuário logado na estação/servidor que originou o tráfego;

2.1.12.2.4. Aplicação;

2.1.12.2.5. Porta de destino;

2.1.12.2.6. IP de origem;

2.1.12.2.7. IP de destino;

2.1.12.2.8. Horário;

2.1.12.2.9. Ação do firewall;

2.1.12.2.10. Severidade;

2.1.12.2.11. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.1.12.2.12. A análise automática deve incluir, no mínimo, as seguintes características:

2.1.12.2.13. Padrões de consulta;

2.1.12.2.14. Entropia;

2.1.12.2.15. Análise de frequência n-gram de domínios;

2.1.12.2.16. Taxa de consultas.

2.1.12.2.17. Deve possuir a capacidade de analisar em tempo real a requisições de DNS e acesso a novas assinaturas de DNS;

2.1.13. SDWAN

2.1.13.1. Deve ser capaz de agregar vários links em uma interface virtual;

2.1.13.2. Deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jiter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras da interface virtual;

2.1.13.3. Deve poder adicionar e equilibrar, no mínimo, 06 interfaces de dados (links e VPNS);

2.1.13.4. Deve suportar a agregação de túneis de VPN IPSec e balancear o tráfego entre eles e inserir essa interface agregada à Interface Virtual;

2.1.13.5. Deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface virtual;

2.1.13.6. Deve possibilitar a distribuição de trafego entre os links que compõe a interface virtual, a critério do administrador;

2.1.13.7. Deve suportar a critério do administrador uma topologia Full-mesh;

2.1.13.8. Deve permitir configurar acesso direto à Internet para aplicações tipo SaaS;

2.1.13.9. Quando ambos os pontos de extremidade dos túneis SD-WAN estiverem ativos, deve haver a duplicação de pacotes (PD) para manter a experiência dos usuários mesmo em condição de perda de pacotes. A duplicação de pacotes deve criar uma cópia do fluxo de tráfego do aplicativo e a enviar em ambos os túneis disponiveis que

está orientado ao mesmo destino.

2.1.13.10. O dispositivo de SD-WAN deve utilizar Forward Error Correction (FEC) habilitado, para permitir que aplicativos sensíveis à perda de pacotes não sejam impactados em caso de perda de pacote e recupere os pacotes perdidos ou corrompidos usando pacotes de paridade incorporados no fluxo da comunicação. O objetivo é reparar o fluxo antes que ele precise fazer failover para outro caminho.

2.1.14. SUPORTE E GARANTIA DO FABRICANTE

2.1.14.1. Deve operar no regime 24/7;

2.1.14.2. Deve ser possivel abrir chamados telefonicos diretamente no fabricante no modelo 24/7;

2.1.14.3. Deve ter um tempo de resposta para chamados críticos de até 1 (uma hora);

2.1.14.4. Em caso de falha de hardware o envio do equipamento para a substituição deve operar no modo NBD (Next Business Day);

2.2. SOFTWARE PARA GERENCIAMENTO CENTRALIZADO DO CLUSTER DE FIREWALLS

2.2.1. O appliance virtual deve ser compatível com VMware ESXi, Microsoft Hyper-V e KVM;

2.2.2. Deve possuir capacidade de armazenamento de até 24TB;

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

2.2.4. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções.

2.2.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

2.2.6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;

2.2.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;

2.2.8. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;

2.2.9. Deve permitir a criação de objetos e políticas compartilhadas;

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

2.2.11. Deve permitir que exportar backup de configuração automaticamente via agendamento;

2.2.12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;

2.2.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;

2.2.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

2.2.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou

WEB (HTTPS) e API aberta;

2.2.16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

2.2.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

2.2.18. O gerenciamento deve permitir/possuir:

- **2.2.18.1.** Criação e administração de políticas de firewall e controle de aplicação;
- **2.2.18.2.** Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- **2.2.18.3.** Criação e administração de políticas de Filtro de URL;
- **2.2.18.4.** Monitoração de logs;
- **2.2.18.5.** Ferramentas de investigação de logs;
- **2.2.18.6.** Debugging;
- **2.2.18.7.** Captura de pacotes.
- **2.2.18.8.** Acesso concorrente de administradores;

2.2.19. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

2.2.20. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

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

2.2.22. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

2.2.23. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

2.2.24. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

2.2.25. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

2.2.26. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.2.27. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

2.2.28. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

2.2.29. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

2.2.30. Criação de regras que fiquem ativas em horário definido;

2.2.31. Criação de regras com data de expiração;

2.2.32. Backup das configurações e rollback de configuração para a última configuração salva;

2.2.33. Suportar Rollback de Sistema Operacional para a ultima versão local;

2.2.34. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

2.2.35. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

2.2.36. Deve suportar interface de configuração baseada no padrão Openconfig.

2.2.37. Validação de regras antes da aplicação;

2.2.38. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

2.2.39. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

2.2.40. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

2.2.41. Deve possuir mecanismo interno ou externo que permita que as configurações ainda não instaladas sejam mantidas mesmo na ocasião de uma reinicialização não esperada.

2.2.42. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

2.2.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

2.2.44. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior;

2.2.45. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

2.2.46. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

2.2.47. Deve ter a capacidade de encaminhar todo tráfego seja ele criptografado ou não para uma cadeia de equipamentos de segurança tais como IPS, IDS e SIEM para inspeção. Esta funcionalidade pode ser entregue por ferramenta externa.

2.2.48. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

2.2.49. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

2.2.50. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

2.2.51. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças

identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

2.2.52. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

2.2.53. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

2.2.54. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

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

2.2.56. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

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

2.2.58. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

2.2.59. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

2.2.60. Deve ser possível exportar os logs em CSV;

2.2.61. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

2.2.62. Rotação do log;

2.2.63. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

2.2.64. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação etc.;

2.2.65. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

- **2.2.65.1.** Situação do dispositivo e do cluster;
- **2.2.65.2.** Principais aplicações;
- **2.2.65.3.** Principais aplicações por risco;
- **2.2.65.4.** Administradores autenticados na gerência da plataforma de segurança;
- **2.2.65.5.** Número de sessões simultâneas;
- **2.2.65.6.** Status das interfaces;
- **2.2.65.7.** Uso de CPU;
- **2.2.65.8.** Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
- **2.2.65.9.** Resumo gráfico de aplicações utilizadas;
- **2.2.65.10.** Principais aplicações por utilização de largura de banda de entrada e saída;
- **2.2.65.11.** Principais aplicações por taxa de transferência de bytes;

2.2.65.12. Principais hosts por número de ameaças identificadas;

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

2.2.66. Deve permitir a criação de relatórios personalizados;

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

2.2.68. Gerar alertas automáticos via:

2.2.68.1. Email;

2.2.68.2. SNMP;

2.2.68.3. Syslog;

2.3. ZERO TRUST NETWORK ACCESS (ZTNA) COM CAPACIDADE PARA SUPORTAR 400 USUÁRIOS

2.3.1. REQUISITOS GERAIS DA SOLUÇÃO

2.3.1.1. A solução de segurança na borda deverá suportar, no mínimo, as seguintes funcionalidades:

2.3.1.1.1. ZTNA (Zero Trust Network Access).

2.3.1.1.2. Filtro de URL;

2.3.1.1.3. Controle de Aplicação;

2.3.1.1.4. Prevenção de Ameaças;

2.3.1.1.5. Solução de segurança DNS;

2.3.1.1.6. Proteção Contra Malwares Modernos (Sandbox);

2.3.1.1.7. Gerência e Relatórios.

2.3.1.2. A solução deverá ser licenciada para permitir a autenticação para acesso de 200 usuários conectados simultaneamente

2.3.1.3. A solução disponibilizada deverá ter capacidade de receber via redirecionamento ou interceptar de maneira ativa e realizar inspeção e tratamento de todo o tráfego web de forma a controlar os acessos a serviços SaaS (Gerenciados e não gerenciados), IaaS, Web e Aplicações Internas (Nuvem pública e on-premises).

2.3.1.4. A solução deve possuir console única de gestão para toda a plataforma de segurança, incluindo:

2.3.1.4.1. Painel de Política;

2.3.1.4.2. Painel de Relatório;

2.3.1.4.3. Painel de Incidentes;

2.3.1.4.4. Painel de Configuração;

2.3.1.4.5. Painel Analítico.

2.3.1.5. O fabricante da solução deverá possuir ao menos 2 gateways no Brasil com pelo menos 2 (dois) endereços IPs dedicados para cada um deles e garantir que as configurações sejam aplicadas aos mesmos localmente, não sendo permitidas soluções genéricas agregadas através de appliances físicos e/ou virtuais;

2.3.1.6. A solução deverá prover às redes remotas faixas de endereços exclusivos para acesso à Internet, saindo apenas com IPs designados para o Brasil.

2.3.1.7. Esta funcionalidade também deverá garantir que a mesma faixa de endereço não seja compartilhada com outros clientes;

2.3.1.8. Deverá ser fornecida com no mínimo, 2 (duas) estruturas de processamento redundantes no território nacional (Brasil)

2.3.1.9. A infraestrutura operacional do fabricante da solução deverá ter as certificações SOC-2 e ISO 27001

2.3.1.10. Deverá ser possível realizar a interceptação do tráfego de várias maneiras distintas, com o intuito de cobrir todo o escopo de alcance aos usuários, para no mínimo as seguintes formas:

2.3.1.10.1. Túnel Seguro (IPSEC ou SSL);

2.3.1.10.2. Integração com plataformas de SDWAN;

2.3.1.10.3. Integração com NGFW/UTM (IPSEC);

2.3.1.10.4. Agente (Windows, Linux e MacOS);

2.3.1.11. Os serviços de segurança devem ser fornecidos de maneira transparente às redes/usuários remotas;

2.3.1.12. A solução deve fornecer a capacidade de associar e atribuir toda a atividade do usuário, usando uma representação de identidade conforme integrações com:

2.3.1.12.1. Active Directory;

2.3.1.12.2. Federação (SSO) utilizando SAML v2.0.

2.3.1.12.3. OpenID Connect/OAuth 2.0

2.3.1.12.4. Suportar recurso de autenticação única para todo o ambiente, utilizando o padrão de autenticação Active Directory, OpenID Connect/OAuth 2.0 ou outra plataforma com suporte à SAML;

2.3.1.13. A solução deverá ser capaz de prover acesso às aplicações internas sem a necessidade de instalação de máquinas virtuais na rede de destino como ponte de acesso;

2.3.1.14. A solução deverá executar suas funcionalidades para defender a rede/usuário contra ameaças avançadas, vírus e ameaças escondidas em tráfego HTTPS e aplicações com SSL criptografado;

2.3.1.15. A solução deverá ser capaz de descriptografar e inspecionar todo o tráfego SSL/TLS, nas versões TLS 1.2 ou superior;

2.3.1.16. O tráfego SSL/TLS deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao tráfego não criptografado;

2.3.1.17. Deverá permitir a configuração de portas diferentes das portas padrão utilizadas pelos protocolos HTTPS/SSL e HTTP, utilizado no acesso de clientes a sites;

2.3.1.18. A solução deverá verificar os certificados digitais de sites acessados por meio do protocolo HTTPS. Em caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência do TJ-CE, bloquear ou permitir o acesso aos sites;

2.3.1.19. Deverá permitir configurar regras de exceção a sites HTTPS que não devem ter seu tráfego inspecionado;

2.3.1.20. O licenciamento e a garantia pelo fabricante para toda a solução deverão estar ativos durante toda a vigência do contrato;

2.3.2. ZTNA (ZERO TRUST NETWORK ACCESS)

2.3.2.1. A solução deve possuir a capacidade de controlar o acesso e aplicar controle de aplicação, proteção contra malwares modernos (Sandbox), prevenção de ameaças e segurança de DNS, de usuários remotos a aplicações internas através da nuvem do fabricante, onde o usuário remoto tenha acesso apenas a aplicação especificada na

política de segurança e não a um segmento de rede interna;

2.3.2.2. A solução deve ser implementada com agente único na estação de trabalho do usuário remoto;

2.3.2.3. Ao se conectar remotamente na solução para acesso a uma aplicação interna, a máquina remota não deve ter acesso, nem ser atribuído em um segmento de rede interna como em um sistema de VPN tradicional;

2.3.2.4. A solução deve garantir acesso seguro a nível de aplicação, ao invés de prover acesso local a rede;

2.3.2.5. Ser possível configurar através da console gráfica da solução quais aplicações internas serão acessadas através do Tenant da solução;

2.3.2.6. Ser autossuficiente e se ajustar automaticamente do ponto de vista de performance caso algum ponto de presença venha a falhar sem a necessidade do administrador ou cliente configurar nenhuma regra;

2.3.2.7. Trabalhar em modo híbrido, onde seja possível publicar os atalhos de acesso a aplicações presentes nos datacenters do TJ-CE e nas nuvens públicas indicadas pela mesma;

2.3.2.8. A solução deve permitir definir a conformidade de estações com sistemas operacionais Windows, Linux e MacOS, com as políticas organizacionais baseadas no mínimo nos seguintes critérios:

2.3.2.8.1. Presença de processo(s) em execução;

2.3.2.8.2. Presença de arquivos em disco;

2.3.2.8.3. Participação em domínio do AD;

2.3.2.8.4. Existência de Certificado Digital no dispositivo;

2.3.2.8.5. Que somente as máquinas que estejam com solução anti-malware ativada possam acessar os serviços internos.

2.3.2.8.6. O cliente SSL client-to-site também deve suportar dispositivos móveis (IOS e ANDROID), sistemas operacionais Linux;

2.3.2.9. A solução deverá permitir o acesso diferenciado para um mesmo usuário conforme as seguintes condições:

2.3.2.9.1. Máquinas em conformidade: A partir de uma máquina remota, com pré-requisitos de segurança identificados, deve permitir o acesso a aplicação;

2.3.2.9.2. Geolocalização: A partir de uma máquina remota tentando se conectar de um país não permitido, deverá ter sua conexão bloqueada;

2.3.2.10. Pela solução deve ser possível criar políticas de segurança onde pode ser especificado:

2.3.2.10.1. Usuário do AD;

2.3.2.10.2. Grupo do AD;

2.3.2.10.3. Aplicação Privada;

2.3.2.10.4. Perfil de segurança (por exemplo: Filtro de URLs, Controle de Aplicação e inspeção Anti-malware);

2.3.2.10.5. Ação: Permitir e/ou Bloquear.

2.3.2.11. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host,

criptografia do disco, chaves de registros e processos ativos;

2.3.2.12. A solução deve realizar verificação contínua de confiança, onde uma vez que o acesso a um aplicativo é concedido;

2.3.2.13. A confiança deverá ser continuamente avaliada com base em mudanças nas condições de segurança na estação;

2.3.2.14. Possuir capacidade de analisar dinamicamente (continuamente) os acessos dos usuários conectados remotamente a internet e recursos do próprio órgão;

2.3.2.15. Suportar políticas de permissão e negação de acesso com base em várias condições. Por exemplo: postura do dispositivo, localização do dispositivo/usuário, associação ao grupo de usuários;

2.3.2.16. Se algum comportamento suspeito for detectado, o acesso pode ser revogado em tempo real;

2.3.2.17. A solução deve gerar logs dos acessos realizados por usuários remotos as aplicações internas, no mínimo, com as seguintes informações:

2.3.2.17.1. Regra de segurança que foi aplicada no tráfego;

2.3.2.17.2. Ação tomada pela solução;

2.3.2.17.3. Usuário;

2.3.2.17.4. Endereço IP;

2.3.2.17.5. IP público e IP privado.

2.3.2.17.6. País de origem;

2.3.2.17.7. Porta de origem;

2.3.2.17.8. Sistema operacional;

2.3.2.17.9. Aplicação de destino;

2.3.2.17.10. Porta de destino;

2.3.2.17.11. Protocolo;

2.3.2.17.12. Bytes trafegados na sessão;

2.3.2.17.13. Hora de início e término da sessão.

2.3.2.18. Deve permitir que a conexão com o serviço SASE seja estabelecida das seguintes formas:

2.3.2.18.1. Antes do usuário autenticar na estação;

2.3.2.18.2. Após autenticação do usuário na estação;

2.3.2.18.3. Sob demanda do usuário;

2.3.2.18.4. Sempre ativo mantendo o usuário conectado assim que o usuário faz o logon.

2.3.2.18.5. A solução deve enviar a lista de gateways ativos para estabelecimento da conexão;

2.3.2.18.6. Deve haver a opção do cliente remoto escolher manualmente o gateway de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

2.3.3. FILTRO DE URLS

2.3.3.1. A solução deverá suportar a criação de políticas baseadas no controle por URL e categorias de URLs;

2.3.3.2. O perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;

2.3.3.3. A solução deverá possuir:

2.3.3.3.1. Pelo menos 70 categorias distintas de URLs;

2.3.3.3.2. A capacidade de classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto;

2.3.3.3.3. Categoria específica para classificar domínios recém registrados (com menos de 30 dias);

2.3.3.3.4. Base contendo, no mínimo, 20 milhões de sites internet web já registrados e classificados com atualização automática;

2.3.3.4. A solução deve possuir, no mínimo, os seguintes atributos para construção de políticas de filtro de conteúdo WEB:

2.3.3.4.1. Categoria de URL;

2.3.3.4.2. Usuários e Grupos do Active Directory;

2.3.3.4.3. Profile de prevenção de malwares;

2.3.3.4.4. Atividade realizada na URL/Aplicação;

2.3.3.4.5. IP de Origem;

2.3.3.4.6. IP de Destino;

2.3.3.4.7. País de origem e destino;

2.3.3.4.8. Ação: allow, block e alert;

2.3.3.4.9. Tipo de arquivo.

2.3.3.4.10. A categorização de URL deverá analisar toda a URL e não somente até o nível de diretório;

2.3.3.5. A solução deverá suportar:

2.3.3.5.1. A criação de categorias de URLs customizadas;

2.3.3.5.2. A exclusão de URLs do bloqueio, por categoria;

2.3.3.5.3. A customização de página de bloqueio;

2.3.3.5.4. A capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local.

2.3.3.6. A solução deverá permitir:

2.3.3.6.1. Um mecanismo para sobrescrever as categorias de URL;

2.3.3.6.2. A criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;

2.3.3.6.3. Especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.3.3.6.4. A solução deverá possuir mecanismo de Controle de URL que apresenta contagem de utilização de regra de acordo com a utilização (hit count);

2.3.3.7. A solução deverá possibilitar:

2.3.3.7.1. Categorização e recategorização de URL caso não esteja categorizada ou categorizada incorretamente;

2.3.3.7.2. A inspeção de tráfego HTTPS Outbound deverá efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo de descriptografia para inspeção completa do tráfego de saída para a internet;

2.3.3.7.3. Implementação de filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das estações dos usuários.

2.3.3.7.4. O cadastro manual de usuários e grupos diretamente na interface de gerência remota;

2.3.3.7.5. 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);

2.3.3.7.6. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

2.3.3.7.7. A solução deverá ser capaz de detectar e prevenir roubo de credenciais, controlando e bloqueando os sites que o usuário pode enviar credenciais corporativas com base na classificação do endereço, em tempo real.

2.3.3.7.8. A solução deverá possuir a capacidade de detectar técnicas de phishing ou falsificação de imagens;

2.3.3.7.9. A solução deverá utilizar modelos de inteligência preditiva no reconhecimento de URLs maliciosas em tempo real não cadastradas na base de categorização do fabricante da solução.

2.3.4. CONTROLE DE APLICAÇÕES

2.3.4.1. A solução deverá possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

2.3.4.2. A solução deverá contar com módulos de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

2.3.4.3. Pela solução deverá ser possível:

2.3.4.3.1. A liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

2.3.4.3.2. A criação de políticas por geolocalização, permitindo que o tráfego de uma aplicação para um determinado país seja bloqueado ou redirecionado;

2.3.4.3.3. Adicionar políticas de controle de aplicações e perfis de segurança para todo o tráfego web e interno através da nuvem SSE, não se limitando somente a possibilidade de habilitar controle de aplicações em parte do tráfego;

2.3.4.3.4. Adicionar controle de aplicações em todas as regras de segurança da solução, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

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

2.3.4.4. A criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

2.3.4.4.1. Nível de risco da aplicação;

2.3.4.4.2. Categoria de aplicações.

2.3.4.4.3. A solução deverá reconhecer pelo menos 3.000 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 webmail;

2.3.4.4.4. A solução deverá suportar múltiplos métodos de

identificação e classificação das aplicações, por pelo menos assinaturas, decoders de protocolos e heurísticas;

2.3.4.5. A solução deverá diferenciar:

2.3.4.5.1. Tráfegos peer-to-peer (bittorrent, emule, neonet, etc.), possuindo granularidade de controle para os mesmos;

2.3.4.5.2. Tráfegos de mensageiros instantâneos (facebook Chat, WhatsApp, telegram e etc.) possuindo granularidade de controle para os mesmos;

2.3.4.5.3. Aplicações proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle para eles.

2.3.4.5.4. A solução deverá diferenciar e controlar partes das aplicações, incluindo, mas não limitado: Permitir o WhatsApp WEB e bloquear a transferência de arquivos, permitir o facebook e bloquear chat;

2.3.4.6. Pela solução deverá ser possível:

2.3.4.6.1. Inspecionar o payload do pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

2.3.4.6.2. Realizar filtragens/inspeções dentro de portas TCP conhecidas, por exemplo porta 80 http, buscando por aplicações que potencialmente expõem o ambiente como: peer-to-peer ou mensageiros instantâneos;

2.3.4.6.3. Identificar o uso de táticas evasivas, ou seja, deverá ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como ataques utilizando comunicação TLS;

2.3.4.6.4. Aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a encrypted bittorrent e aplicações VOIP que utilizam criptografia proprietária.

2.3.4.6.5. Caso a solução não tenha assinaturas pré-definidas de uma aplicação, ela deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, HTTPS, FTP, E-mail e extensão de arquivos;

2.3.4.6.6. Pela solução deverá ser possível atualizar a base de assinaturas de aplicações automaticamente;

2.3.4.6.7. O fabricante da solução deverá disponibilizar um serviço para solicitação de inclusão de aplicações na base de assinaturas dele;

2.3.5. PREVENÇÃO DE AMEAÇAS

2.3.5.1. A solução deverá proteger o acesso do usuário aos dados corporativos, controlando a exposição dos mesmos quanto à movimentação entre nuvens (SaaS Gerenciado e SaaS não gerenciado);

2.3.5.2. Na solução deverá ser possível criar políticas de segurança baseadas no nível de risco da aplicação. Ex: selecionar na política de segurança o bloqueio de todas as aplicações de cloud storage com nível de risco alto na base do fabricante da solução;

2.3.5.3. Deve conter, no mínimo, as seguintes informações sobre as

aplicações comparadas na interface gráfica da solução:

2.3.5.3.1. Informações sobre vulnerabilidades e exploits já sofridos;

2.3.5.3.2. Certificações e normas que a aplicação está aderente. Ex: PCI, DSS, SOC-1, SOC-2 e SOC-3;

2.3.5.3.3. Informações sobre privacidade de dados. Ex: ao armazenar dados na aplicação, o cliente continua sendo proprietário dos dados.

2.3.5.3.4. A solução deverá possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;

2.3.5.4. A solução deverá suportar:

2.3.5.4.1. Várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

2.3.5.4.2. Referência cruzada com CVE.

2.3.5.5. A solução deverá ser capaz de categorizar os seguintes tipos de domínio:

2.3.5.5.1. Domínios de DNS dinâmicos;

2.3.5.5.2. Domínios identificados previamente como sendo distribuidores de Malwares;

2.3.5.5.3. Domínios identificados anteriormente em campanhas de Phishing;

2.3.5.5.4. Domínios identificados previamente como Graywares os quais podem usar de técnicas de instalação de aplicações não desejadas;

2.3.5.5.5. Domínios Estacionários os quais são sites com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares;

2.3.5.5.6. Domínio de anonimização de Proxy utilizados com uma forma de driblar a análise de conteúdo.

2.3.5.5.7. A solução deverá possuir sistema de análise automática para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.3.5.5.8. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning), e impedir que os usuários acessem endereços de domínios bloqueados ou maliciosos;

2.3.5.5.9. A solução deverá permitir updates em tempo real para ameaças e novos ataques feitos através de DNS.;

2.3.6. SEGURANÇA DNS

2.3.6.1. A solução de segurança de DNS, tem como finalidade proteger as conexões a domínios maliciosos que muitas vezes são utilizados pelos atacantes, utilizam para interceptar a comunicação e poder ter acesso e controlar a comunicação dos usuários, causando problemas de evasão e exfiltração de dados;

2.3.6.2. Caso o fabricante não tenha solução de segurança para DNS de forma nativa, ou seja, licenciada de forma separada da solução, o mesmo pode compor com outra solução dedicada de mercado de fabricantes como (ex.: Cisco Umbrella) e deverá ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.6.3. A solução de segurança de DNS deve ser capaz de identificar

atividades maliciosas de comando e controle utilizado pelo menos as seguintes técnicas:

2.3.6.4. A solução deve mostrar nos logs as seguintes informações sobre domínios DGA:

2.3.6.4.1. Domínio suspeito identificado;

2.3.6.4.2. ID de assinatura de detecção;

2.3.6.4.3. Usuário logado na estação/servidor que originou o tráfego;

2.3.6.4.4. Aplicação;

2.3.6.4.5. Porta de destino;

2.3.6.4.6. IP de origem;

2.3.6.4.7. IP de destino;

2.3.6.4.8. Horário;

2.3.6.4.9. Ação do firewall;

2.3.6.4.10. Severidade;

2.3.6.4.11. A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle;

2.3.6.5. A análise automática deve incluir, no mínimo, as seguintes características:

2.3.6.5.1. Padrões de consulta;

2.3.6.5.2. Entropia;

2.3.6.5.3. Análise de frequência n-gram de domínios;

2.3.6.5.4. Taxa de consultas.

2.3.6.5.5. A solução deve permitir updates em tempo real para ameaças e novos ataques feitos através de DNS;

2.3.6.5.6. A solução deve permitir a utilização ilimitada (quantidades) de assinaturas DNS;

2.3.6.6. A solução de segurança de DNS deve ser capaz de categorizar os seguintes tipos de domínio:

2.3.6.6.1. Domínios de DNS dinâmicos

2.3.6.6.2. Domínios identificados previamente como sendo distribuidores de malwares

2.3.6.6.3. Domínios registrados recentemente

2.3.6.6.4. Domínios identificados anteriormente em campanhas de phishing

2.3.6.6.5. Domínios identificados previamente como graywares os quais podem usar de técnicas de instalação de aplicações não desejadas

2.3.6.6.6. Domínios Estacionários os quais são sítios com conteúdo limitado e que podem ser utilizados como um ponto de distribuição de malwares.

2.3.6.6.7. Domínio de proxy de animação utilizados com uma forma de driblar a análise de conteúdo.

2.3.7. PROTEÇÃO CONTRA MALWARES MODERNOS

2.3.7.1. A solução deverá possuir nuvem de inteligência proprietária do fabricante que seja responsável em atualizar toda a base de segurança através de assinaturas;

2.3.7.2. A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise em tempo real em uma sandbox, devendo

permitir a análise na nuvem do fabricante da solução, onde o arquivo será executado e simulado em ambiente controlado (sandbox). Caso esta funcionalidade seja licenciada de forma separada da solução, deverão ser fornecidas todas as licenças necessárias para a utilização desta funcionalidade.

2.3.7.3. A solução deverá prevenir o uso de exploits avançados;

2.3.7.4. Na solução, a análise deverá prover:

2.3.7.4.1. Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

2.3.7.4.2. Informações sobre as ações do malware na máquina infectada;

2.3.7.4.3. Informações sobre as URLs não confiáveis utilizadas pelo novo malware;

2.3.7.4.4. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção;

2.3.7.4.5. Detecção de aplicações não confiáveis, utilizadas pelo Malware;

2.3.7.4.6. Assinaturas de antivírus e antispyware de maneira automática.

2.3.7.5. A solução deverá possuir:

2.3.7.5.1. Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS;

2.3.7.5.2. Mecanismo de detecção "antibot", que inclui pelo menos, reputação de endereço IP;

2.3.7.5.3. Funcionalidade de detecção e bloqueio de call-backs.

2.3.7.5.4. A solução deverá prevenir contra ameaças de dia zero:

2.3.7.5.5. Via tráfego de internet;

2.3.7.5.6. Que possam burlar o sistema operacional emulado;

2.3.7.5.7. Através de tecnologias em nível de emulação e código de registro.

2.3.7.5.8. A solução deverá ser capaz de implementar:

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

2.3.7.5.8.2. Visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

2.3.7.5.8.3. Análise de arquivos executáveis, DLLs e ZIP em SSL no ambiente controlado;

2.3.7.5.9. A solução deverá suportar ainda:

2.3.7.5.9.1. Identificação e bloqueio de malware nas comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

2.3.7.5.9.2. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs, MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

2.3.7.5.9.3. Suportar a análise dinâmica de arquivos

maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows 10, Mac OS X, iOS, Android e Linux;

2.3.7.5.9.4. A solução deve analisar os arquivos do tipo malware em bare-metal para evitar técnicas de evasão. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função;

2.3.8. SUPORTE E GARANTIA DO FABRICANTE

2.3.8.1. O Serviço deverá fornecer:

2.3.8.1.1. Acesso a Especialistas Técnicos e Recursos Online:

2.3.8.1.1.1. A solução deverá fornecer acesso imediato a especialistas técnicos e recursos online, garantindo proteção ao produto oferecido. Os usuários poderão submeter, atualizar e verificar o status dos casos de suporte por meio de um Portal de Suporte ao Cliente online.

2.3.8.2. Transferência de Conhecimento Avançada:

2.3.8.2.1. A solução incluirá uma plataforma completa de transferência de conhecimento. Isso abrangerá documentação detalhada do produto, bancos de dados de resolução de problemas e um ambiente de gerenciamento de casos de suporte baseado em conhecimento, permitindo colaboração entre usuários. Além disso, serão disponibilizados manuais de produtos, guias técnicos, notas de lançamento de software e FAQs para simplificar a resolução de incidentes.

2.3.8.3. Serviço de Melhoria Contínua:

2.3.8.3.1. A solução oferecerá um serviço de melhoria contínua para maximizar o valor do produto. Isso incluirá o desenvolvimento de planos de sucesso personalizados, alinhados com metas e requisitos específicos da organização. Serão realizadas verificações periódicas da saúde da solução e aplicadas as melhores estratégias de utilização para otimização e proteção do investimento.

2.3.8.4. Integração de Fluxos de Trabalho Operacionais:

2.3.8.5. A solução garantirá a integração eficaz com fluxos de trabalho operacionais. A equipe especializada colaborará com a infraestrutura de rede e segurança, identificando pontos de integração, conduzindo verificações regulares e revisões operacionais para promover uma operação mais eficiente e aumentar a confiança na solução.

2.3.8.6. Os SLAs de para tempos de resposta, deverão obedecer aos seguintes níveis de severidade:

Severidade	Descrição	SLA
1	Grave impacto no ambiente de produção, como a perda de dados de produção ou a inoperância de sistemas.	Até 1 hora, contada a partir do registro do chamado.
2	O software opera, porém, seu desempenho em no ambiente de produção é consideravelmente limitado.	Até 2 horas, contadas a partir do registro do chamado.
3	Perda parcial e não crítica de funcionalidade de software no ambiente de produção, mas é viável continuar usando-o por meio de uma	Até 4 horas, contadas a partir do registro do chamado.

	solução alternativa	
4	Questionamento de natureza geral, notificação de discrepância na documentação ou sugestão de aprimoramento ou alteração do produto.	Até 48 horas, contadas a partir do registro do chamado.

2.4. INSTALAÇÃO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.4.1. É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e componentes da solução ofertada. Os equipamentos e componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou componente de hardware fora das condições normais recomendadas pelo fabricante.

2.4.2. A Contratada deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off no intuito de revisar os requisitos do projeto, discutir cronogramas de marcos do projeto, membros da equipe e itens de ação de acompanhamento.

2.4.3. Deverá conduzir através de um workshop uma sessão de design profundada do cenário da implantação da solução através da colaboração das principais partes interessadas da contratante no intuito de desenvolver e concordar com os critérios de design e a estratégia de implantação;

2.4.4. Os serviços de instalação e configuração, compreendem, entre outros, os seguintes procedimentos:

2.4.4.1. Análise da topologia e arquitetura da rede, considerando os roteadores, servidores de aplicação e firewall já existentes e instalados;

2.4.4.2. Análise do acesso Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

2.4.4.3. Regras de Firewall existentes e aplicáveis à solução ofertada dada a colocação desta na Rede deste parque;

2.4.4.4. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

2.4.4.5. Apresentação do plano de implantação com o descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;

2.4.4.6. A realização dos ajustes de hardware e software necessários ao funcionamento dos equipamentos;

2.4.4.7. Aplicação de todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;

2.4.4.8. Configuração do sistema de Firewall, VPN, IPS, Filtro URL, Antivírus e Anti-Malware de acordo com as exigências levantadas com as devidas atualizações necessárias;

2.4.4.9. Instalação de Sistema de Gerência Centralizada em Appliance Físico, Appliance Virtual ou solução baseada em VM (máquina virtual), de acordo com a oferta da CONTRATADA. O mesmo será

considerado entregue, quando for instalado e configurado, com todas as atualizações, configurações e licenças ativadas. Deverão ser adicionados ao Sistema de Gerência Centralizada todos os equipamentos instalados contemplados na solução adquirida. Os equipamentos deverão ser monitorados e gerenciados por este Sistema de Gerência Centralizada;

2.4.4.10. Habilitação das licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados pela solução;

2.4.4.11. Inclusão de políticas de segurança encaminhadas pelo CONTRATENTE, pré-existentes em seu ambiente, para os novos equipamentos.

2.4.5. A CONTRATADA deverá, ao final dos trabalhos, fornecer a entrega da documentação técnica completa da solução, contendo:

2.4.5.1. Os procedimentos de instalação e configuração,

2.4.5.2. Cenário de implantação e integração da rede;

2.4.5.3. Diagrama/documentação de rede para referência;

2.4.5.4. Lista de materiais/inventário da solução;

2.4.5.5. Versão do Sistema Operacional;

2.4.5.6. Hardening/segurança do sistema;

2.4.5.7. Capacidades fundamentais;

2.4.5.8. Requisitos específicos do cenário de implantação;

2.4.5.9. Detalhes de design de baixo nível (por exemplo, endereços IP, nomes de dispositivos, matriz de cabeamento, pesquisa do local, configuração específica do site/dispositivo);

2.4.5.10. Estratégia de validação - principais pontos de verificação a serem testados;

2.4.5.11. Bem como fornecer um repasse sobre a solução e as configurações realizadas.

2.5. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.5.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.1.14, durante todo o período de vigência do contrato.

2.5.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.5.2.1. Suporte técnico para identificação e resolução de problemas em software e hardware;

2.5.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.5.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.5.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.5.2.6. Encaminhar incidentes ao fabricante da solução;

2.5.2.7. Suporte em demais configurações de segurança, redundância e

gerência;

2.5.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.5.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.5.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.5.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.5.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.5.2.13. O suporte linguístico fornecido pela contratada deve assegurar que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.5.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.5.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.5.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.5.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.5.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.5.2.19. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.5.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de

Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.5.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

2.5.2.22. A CONTRATADA deverá executar a cada 3 meses e apresentar os resultados encontrados incluindo sugestão de ações de melhoria para serem executadas, Assessments de boas práticas e de revisão de ciclo de vida de segurança, que possam resumir riscos operacionais e de segurança do TJCE, bem como a aderência a melhores práticas e configurações recomendadas pelo fabricante.

2.6. TREINAMENTO PARA NEXT GENERATION FIREWALL EM ALTA DISPONIBILIDADE

2.6.1. Deverá fornecer treinamento para até 8 (oito) alunos, a fim de capacitar os profissionais da CONTRATANTE;

2.6.2. O serviço de capacitação deve consistir na oferta de treinamentos com abordagem prática voltada a todos os requisitos funcionais da solução contratada, tanto relativo a aspectos operacionais, que inclui a utilização prática de todas as principais funcionalidades da ferramenta, como administrativos, que inclui o gerenciamento, suporte e parametrização da solução.

2.6.3. Ministrado por profissionais da CONTRATADA com conhecimentos comprovados na solução oferecida.

2.6.4. Deve incluir fornecimento de documentação didática em papel ou mídia digital com todo o conteúdo.

2.6.5. Deve ser composto por parte teórica e prática, com uso de laboratórios virtuais da CONTRATADA ou do fabricante.

2.6.6. O treinamento deve abordar, no mínimo, os seguintes tópicos:

2.6.6.1. Conceitos, configuração, gerenciamento e diagnóstico de problemas;

2.6.6.2. Arquitetura e Componentes do NGFW;

2.6.6.3. Sistema de Prevenção de Intrusão;

2.6.6.4. Políticas de Segurança e Aplicações;

2.6.6.5. Filtragem de Conteúdo, Aplicações e URL;

2.6.6.6. Balanceamento de Carga e Alta Disponibilidade;

2.6.6.7. Relatórios, Conformidade e Regulamentações;

2.6.6.8. Customização de Relatórios e Monitoramento;

2.6.6.9. Gerenciamento de Usuários e Autenticação;

2.6.6.10. Registros de eventos;

2.6.6.11. Registro de tráfego;

2.6.6.12. Proteção contra Malware;

2.6.6.13. Controle de Acesso e VPN;

2.6.6.14. Balanceamento de Carga e Alta Disponibilidade;

2.6.6.15. Melhores Práticas de Segurança;

2.6.6.16. Atualizações e Manutenção;

2.6.6.17. Teste de Intrusão e Avaliação de Segurança;

2.6.6.18. Backup e Recuperação de Desastres;

2.6.6.19. Integração com Outras Soluções.

2.6.7. A CONTRATADA poderá incluir tópicos e funcionalidades que julgar necessários, além dos elencados acima;

2.6.8. Após o treinamento, a CONTRATADA deve fornecer certificados de participação a cada funcionário participante, incluindo tópicos abordados, duração e instrutores.

2.6.9. Custos de deslocamento, hospedagem e alimentação dos treinandos são de responsabilidade da CONTRATANTE.

2.6.10. A CONTRATADA será o responsável pela preparação do local de treinamento inclusive da disponibilização e instalação de todos os equipamentos.

2.6.11. A duração mínima do treinamento (carga horária) será de 40 (quarenta) horas em 10 (dez) dias;

2.6.12. O curso deverá ser ministrado em língua portuguesa com o material didático utilizado e fornecido preferencialmente em língua portuguesa.

2.7. INSTALAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.7.1. A Contratada deverá realizar a implementação em conjunto com o fabricante realizando a instalação, configuração e funcionamento dos componentes da solução ofertada. Os componentes serão implementados pela CONTRATADA de acordo com os termos deste TR. Não serão admitidos configurações e ajustes que impliquem no funcionamento fora das condições normais recomendadas pelo fabricante.

2.7.2. Este serviço deverá inclui quatro (4) etapas: Implantação, Integração, Repasse de Conhecimento e Documentação;

2.7.3. A Contratada em conjunto com o fabricante deverá em conjunto com a contratante realizar atividades de planejamento e uma call de Kick-off para realizar o lançamento inicial do projeto. Esta reunião incluir uma revisão dos requisitos do projeto e uma discussão sobre cronogramas e plano de ação;

2.7.4. Após o kick-off, a Contratada em conjunto com o fabricante deverá gerar um Documento de Requisitos Técnico, baseado no ambiente do cliente

2.7.5. O Documento de Requisitos Técnicos descreverá o ambiente de produção planejado e os procedimentos operacionais;

2.7.6. A Contratada em conjunto com o fabricante deverá:

2.7.6.1. Realizar a configuração com base nos requisitos definidos no Documento de Requisitos Técnicos. As tarefas de configuração devem incluir no mínimo:

2.7.6.1.1. Implantação de usuários móveis;

2.7.6.1.2. Conector ZTNA (Configuração e integração de 4 conectores com até 10 alvos de aplicativos);

2.7.6.1.3. Dez (10) políticas de segurança.

2.7.6.2. Revisar e validar a implantação de acordo com os critérios

definidos no Documento de Requisitos Técnicos, apoiando a integração inicial de usuários móveis e validando o comportamento e a conectividade dos usuários, através de um Teste Piloto de Integração

2.7.6.2.1. No Teste Piloto de Integração deverão ser revisados e os registros de tráfego e ameaças e os fluxos de tráfego e garanta que os usuários possam alcançar os destinos adequados definidos pelas políticas de segurança

2.7.6.3. Realizar uma sessão de transferência de conhecimento após a conclusão dos serviços de planejamento, configuração e validação listados acima;

2.7.6.4. Realiza uma sessão de Transferência de Conhecimento deverá incluir uma descrição do ambiente as-built e uma transferência de conhecimento sobre como gerenciar e operar o ambiente. A transferência de conhecimento deverá ser realizada em uma única sessão de até duas (2) horas, para oito (8) participantes;

2.8. SUPORTE TÉCNICO E MONITORAMENTO 24X7 PARA SOLUÇÃO DE ZERO TRUST NETWORK ACCESS (ZTNA)

2.8.1. O serviço de suporte técnico da CONTRATADA deverá ser contínuo na modalidade 24x7, e quando necessário realizando a intermediação com o serviço oficial de garantia e suporte do fabricante da solução, nos moldes descritos no item 2.3.8, durante todo o período de vigência do contrato.

2.8.2. O serviço de suporte técnico e monitoramento 24x7 da CONTRATADA incluirá:

2.8.2.1. Suporte técnico para identificação e resolução de problemas em software;

2.8.2.2. Resolução de problemas quanto acesso à sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

2.8.2.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

2.8.2.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos a solução ofertada;

2.8.2.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

2.8.2.6. Encaminhar incidentes ao fabricante da solução;

2.8.2.7. Suporte em demais configurações de segurança, redundância e gerência;

2.8.2.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

2.8.2.9. Apoio técnico para tarefas de auditoria e análise de logs.

2.8.2.10. Lançamentos de recursos e atualizações de software mais recentes;

2.8.2.11. Atualização dos serviços de assinatura de segurança manual ou automática;

2.8.2.12. Caso o fabricante se comunique e/ou documente em uma língua diferente do português, será de responsabilidade da contratada fornecer suporte linguístico para garantir a compreensão adequada de todas as informações pertinentes ao cumprimento deste contrato.

2.8.2.13. O suporte linguístico fornecido pela contratada deve assegurar

que todas as comunicações e documentos sejam devidamente traduzidos para o idioma acordado pelas partes, garantindo assim uma comunicação clara e precisa entre as partes envolvidas no contrato.

2.8.2.14. As despesas associadas ao fornecimento do suporte linguístico serão de responsabilidade da contratada

2.8.2.15. A CONTRATANTE poderá solicitar qualquer relatório da solução a qualquer tempo, sem restrição de quantidade de solicitações, o que deverá ser provido pela contratada num prazo de 5 dias úteis, contados a partir da data de solicitação por parte da CONTRATANTE

2.8.2.16. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva.

2.8.2.17. O atendimento e suporte técnico especializado será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

2.8.2.18. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

2.8.2.19. A atualização de software quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

2.8.2.20. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

2.8.2.21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional, registro de ameaças e vulnerabilidades identificadas em softwares dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

ANEXO II DO CONTRATO

TERMO DE CIÊNCIA

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ANEXO II - TERMO DE CIÊNCIA

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no _____ sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no CONTRATANTE.

CIÊNCIA
CONTRATADA – Funcionários

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

Termo de Ciência – TCI

_____
<Nome>
Matrícula: *<Matr.>*

_____
<Nome>
Matrícula: *<Matr.>*

_____,_____ de _____ de 20_____.

ANEXO III DO CONTRATO

TERMO DE COMPROMISSO

ESTADO DO CEARÁ
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

ANEXO III - TERMO DE COMPROMISSO – TC

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado em Av. General Afonso Albuquerque Lima, S/N. – Cambeba, Fortaleza-CE CEP:60822-325 – Fone: (85) 3207-7000, CNPJ n° 09.444.530/0001-01, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____, nº _____, _____, _____/__, CEP: __.___-___, CNPJ n° ___.___.___/____-__, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º __/20__ doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da

informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis,

conforme Art. 156 da Lei nº. 14.133/21.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro de Fortaleza-CE, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

Termo de Compromisso

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ Matrícula:	_____ Representante Legal
Testemunhas	
Testemunha 1	**Testemunha 2**
_____ Preposto da Contratada	_____ Fiscal Técnico

_____, _____ de _____ de 20____

ANEXO IV DO CONTRATO
PROPOSTA DA CONTRATADA

(Inserir proposta ajustada ao valor homologado)

ANEXO V DO CONTRATO

FICHA DE DADOS DO REPRESENTANTE LEGAL

Dados pessoais do(s) representante(s) e/ou procurador(es), devidamente habilitados, da futura CONTRATADA, indicado(s) para assinatura do Termo de Contrato:

NOME : _____

NACIONALIDADE : _____

ESTADO CIVIL : _____

PROFISSÃO : _____

RG : _____

CPF : _____

DOMICÍLIO : _____

CIDADE : _____

UF : _____

FONE : _____

FAX : _____

CELULAR : _____

E-MAIL : _____