CONTRATO PARA AQUISIÇÃO DE EQUIPAMENTOS E PROGRAMAS DE DATACENTER, QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, E A EMPRESA PTLS SERVIÇOS DE TECNOLOGIA E ASSESSORIA TÉCNICA LTDA**.**

CONTRATO Nº 029/2022

A UNIÃO, por intermédio do **TRIBUNAL REGIONAL ELEITORAL DA BAHIA,** com sede na 1ª Avenida do Centro Administrativo da Bahia, n.º 150, Salvador - BA, inscrito no CNPJ/MF sob o n.º 05.967.350/0001-45, doravante denominado **Contratante,** neste ato representado por seu Diretor-Geral, **Raimundo de Campos Vieira**, no uso da competência que lhe é atribuída pelo Regulamento Interno da Secretaria do TRE-BA, e a empresa **PTLS SERVIÇOS DE TECNOLOGIA E ASSESSORIA TÉCNICA** LTDA, inscrita no CNPJ/MF n.º 09.162.855/0005-17, com sede na Avenida das Nações Unidas, 12.901, Conjunto N-1802, 18º andar, Torre Norte, Centro Empresarial Nações Unidas (CENU), Brooklin Paulista, São Paulo/SP, CEP: 04.578-910, telefone n.º (11) 3573-3147, e-mail br.tributario@la.logicalis.com, representada neste ato pelo Sr. Herbert José Azevedo, portador da Carteira de Identidade n.º 20.033.911-4 SSP/SP, inscrito no CPF/MF sob n.º 102.603.658-58, e Sr. Fábio Cunha, portador da Carteira de Identidade n.º 21395369 SSP/SP, inscrito no CPF/MF sob n.º 273.389.228-29, resolvem celebrar o presente **CONTRATO PARA AQUISIÇÃO DE EQUIPAMENTOS E PROGRAMAS DE DATACENTER**, albergado na Lei n.º 8.666/93 e alterações, resultante do **Pregão n.º 02/2022**, consoante Processos (SEI) n.º 0015838-60.2021.6.05.8000 e 0006073-31.2022.6.05.8000.

CLÁUSULA PRIMEIRA – *DO OBJETO*

1. O objeto do presente contrato é a aquisição de equipamentos e programas de datacenter**,** conforme as condições estabelecidas no Edital de Pregão n.º 02/2022 e na proposta firmada pela Contratada, que passam a integrar este instrumento, independentemente de transcrição.

CLÁUSULA SEGUNDA - *DO VALOR E DO REAJUSTE CONTRATUAL*

Item	Descrição	Unidade de Fornecimento	Quant.	Valor Unitário	Valor Total
5	Appliance Virtual de Balanceamento de Carga com Firewall de Aplicações. As especificações detalhadas constam no Anexo A do	unidade	02	R$ 498.000,00	**R$ 996.000,00**

	Termo de Referência.				

1. O valor total do presente contrato é de R$ **996.000,00 (novecentos e noventa e seis mil reais)**.

2. O valor acima referido inclui todos os custos diretos e indiretos, bem como deveres, obrigações e encargos de qualquer natureza, não sendo devido à Contratada qualquer outro pagamento resultante da execução deste ajuste.

REAJUSTE

3. Os preços pactuados serão reajustados, observado o interregno mínimo de um ano, a contar da data de apresentação da proposta, aplicando-se a variação do IPCA, calculado e divulgado pelo IBGE.

4. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação em vigor, à época.

5. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial para reajustamento dos preços.

6. Caso os preços contratados, após o cálculo referente ao reajuste citado no item anterior, venham a ser superiores aos praticados no mercado, as partes deverão rever os preços para adequá-los às condições existentes no início do contrato firmado.

CLÁUSULA TERCEIRA – *DA DOTAÇÃO ORÇAMENTÁRIA*

1. A despesa correrá à conta do elemento 3.44.90.40.05 "Aquisição de software Pronto", vinculado à Ação 02.122.0033.20GP.0029 "Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral no Estado da Bahia", do Programa de Gestão e Manutenção do Poder Judiciário".

2. Para a cobertura das despesas, foi emitida a Nota de Empenho n.º 2022NE575, em 2 de maio de 2022.

CLÁUSULA QUARTA – *DA ENTREGA E DO RECEBIMENTO*

1. A entrega e o recebimento do objeto contratado serão efetuados em conformidade com o disposto no Termo de Referência, Anexo I, do Edital, que passa a integrar este instrumento contratual.

2. No momento da entrega, será exigida a comprovação da origem dos bens importados e da quitação dos tributos de importação a eles referentes, sob pena de rescisão contratual e multa.

CLÁUSULA QUINTA – *DAS OBRIGAÇÕES DA CONTRATANTE*

1. A Contratante obriga-se a:

a) acompanhar e fiscalizar a execução do ajuste, anotando em registro próprio as ocorrências acaso verificadas, determinando o que for necessário à regularização das faltas ou defeitos observados;

b) prestar esclarecimentos que venham a ser solicitados pela Contratada;

c) efetuar os pagamentos nas condições e nos prazos constantes dos instrumentos convocatório e contratual;

d) zelar para que, durante a vigência do Contrato, a Contratada cumpra as obrigações assumidas, bem como sejam mantidas as condições de habilitação e qualificação exigidas no processo licitatório;

e) determinar a reparação, a correção, a remoção, a reconstrução ou a substituição do objeto contratado que apresentar vícios ou incorreções resultantes da execução ou de materiais empregados ou do seu uso correto, que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor.

CLÁUSULA SEXTA – *DAS OBRIGAÇÕES DA CONTRATADA*

1. São obrigações da Contratada, além daquelas explícita ou implicitamente contidas no presente Contrato, no Termo de Referência e na legislação vigente:

a) entregar os bens no prazo, nas especificações e na quantidade constantes neste contrato, assim como com as características descritas na proposta;

b) atender às solicitações da Contratante nos prazos estabelecidos neste instrumento;

c) não fornecer quantidade ou modelo diverso do solicitado;

d) substituir os produtos danificados em razão de transporte, descarga ou outra situação que não possa ser imputada à Administração;

e) responder pelos encargos previdenciários, trabalhistas, fiscais e comerciais resultantes da execução deste Contrato;

f) responder por quaisquer danos pessoais ou materiais causados por seus empregados à Administração e/ou a terceiros na execução deste Contrato;

g) manter, durante a execução do ajuste, todas as condições de habilitação exigidas para a contratação;

h) reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto contratado que apresentar vícios ou incorreções resultantes da execução ou de materiais empregados ou do seu uso correto, que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor;

i) não subcontratar, ceder ou transferir, no todo ou em parte, o objeto deste contrato;

j) conferir garantia de adequação dos produtos (qualidade, segurança, durabilidade e desempenho), em conformidade com as condições estabelecidas no Termo de Referência, anexo deste Contrato.

CLÁUSULA SÉTIMA – *DO PAGAMENTO*

1. O pagamento será efetuado na forma e prazo estabelecidos no Termo de Referência, anexo deste Contrato.

2. Por ocasião do pagamento, deverá ser verificada a regularidade da Contratada perante a Fazenda Nacional (Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União), o Fundo de Garantia do Tempo de Serviço (Certificado de Regularidade do FGTS – CRF), a Justiça Trabalhista (Certidão Negativa de Débitos Trabalhistas - CNDT) e a Fazenda Estadual/Distrital (Certidão de Quitação de Tributos Estaduais/Distritais ou Certidão que comprove a regularidade com o ICMS, emitida pelo órgão competente).

3. A Contratada indicará na nota fiscal/fatura o nome do Banco e os números da agência e da conta corrente para efetivação do pagamento.

4. Observados os princípios do contraditório e da ampla defesa, a Contratante poderá deduzir os valores correspondentes a multas, ressarcimentos ou indenizações, devidos pela Contratada, do montante a ser-lhe pago.

5. No caso de atraso de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, serão devidos pela Contratante encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

CLÁUSULA OITAVA – *DA VIGÊNCIA*

1. O contrato terá vigência de 60 (sessenta) meses, contados da data da sua assinatura.

CLÁUSULA NONA – DAS SANÇÕES PELO DESCUMPRIMENTO DAS OBRIGAÇÕES CONTRATUAIS

1. De acordo com o disposto no art. 7º da Lei nº 10.520/2002, ficará IMPEDIDA DE LICITAR E DE CONTRATAR com a União e será descredenciada do SICAF e dos sistemas de cadastramento de fornecedores do TRE-BA, PELO PRAZO DE ATÉ 5 (CINCO) ANOS, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantidos o contraditório e a ampla defesa, a licitante que:

a) não mantiver a proposta, injustificadamente;

b) comportar-se de modo inidôneo;

c) fizer declaração falsa;

d) cometer fraude fiscal;

e) falhar ou fraudar na execução do contrato;

f) não encaminhar documentação exigida no certame ou entregar documentação falsa;

g) não fornecer o objeto licitado;

h) retardar a entrega do objeto licitado;

i) fornecer material que não atenda à especificação exigida no edital.

2. Para os fins da alínea "b", reputar-se-ão inidôneos atos como os descritos nos arts. 90, 92, 93, 94, 95 e 97 da Lei nº 8.666/93.

3. A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas.

4. Qualquer penalidade somente poderá ser aplicada mediante processo administrativo, no qual se assegurem a prévia defesa e o contraditório, consoante rito estabelecido no art. 87, § 2º da Lei 8.666/93, aplicando-se, subsidiariamente, a Lei nº 9.784/99 e a Portaria nº 305/2019, da Presidência do TRE-BA.

5. Pelo inadimplemento total ou parcial das obrigações assumidas, a Contratada estará sujeita à multa prevista no Termo de Referência, Anexo deste Contrato.

6. A Contratante poderá reter dos pagamentos devidos à Contratada, como medida cautelar, independentemente de sua manifestação prévia, valor relativo a eventual multa a ser aplicada em razão de inadimplemento contratual, com base no artigo 45 da Lei nº 9.784/99 e no artigo 26, § 1º, da Portaria nº 305/2019, da Presidência do TRE/BA.

7. O valor da multa aplicada será descontado dos pagamentos eventualmente devidos à licitante vencedora ou da garantia prestada, quando houver, ou ainda, quando for o caso, cobrado judicialmente.

8. Aplicada a penalidade de multa, após regular processo administrativo, observado o disposto nos **itens 6 e 7, desta Cláusula**, será a Contratada, se for o caso, intimada para efetuar o recolhimento do seu valor por meio de Guia de Recolhimento da União – GRU, no prazo de 30 dias, contados da intimação.

9. As situações mencionadas nos incisos I a XII, XVII e XVIII do art. 78 da Lei 8.666/93 podem ensejar, a critério da Administração, a rescisão unilateral do contrato.

10. Os recursos contra a aplicação de sanções em decorrência de inadimplemento contratual serão dirigidos à Presidência do TRE-BA, sendo interpostos na forma e nos prazos estabelecidos no art.109 da Lei 8.666/93.

CLÁUSULA DÉCIMA– *DA ALTERAÇÃO DO CONTRATO*

1. Este contrato poderá ser alterado nos casos previstos no art. 65 da Lei 8.666/93, com a apresentação das devidas justificativas.

CLÁUSULA DÉCIMA PRIMEIRA – *DA RESCISÃO CONTRATUAL*

1. A inexecução total ou parcial do Contrato enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei 8.666/93, sem prejuízo da aplicação das penalidades aqui estabelecidas.

2. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA SEGUNDA– *DA PUBLICAÇÃO*

1. O presente contrato será publicado, em extrato, no Diário Oficial da União, conforme prescreve o art. 61, parágrafo único, da Lei 8.666/93.

CLÁUSULA DÉCIMA TERCEIRA – *DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – LEI 13709/18*

1. O TRE-BA e a Contratada se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, atuando da seguinte forma:

a) a coleta de dados pessoais indispensáveis à própria prestação do serviço, se houver, será realizada mediante prévia e fundamentada aprovação do TRE-BA, responsabilizando-se a Contratada por obter o consentimento dos titulares (salvo nos casos em quer opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins;

b) encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a Contratada providenciará seu descarte de forma segura.

2. A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas neste item, inclusive no tocante à Política de Privacidade do TRE-BA, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

3. O eventual acesso, pela Contratada, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio implicará para a mesma e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

4. Representante da Contratada manterá contato formal com representante do TRE-BA, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação

de dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes.

5. A critério do TRE-BA, a Contratada poderá ser provocada a preencher um relatório de impacto, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

CLÁUSULA DÉCIMA QUARTA – *DO FUNDAMENTO LEGAL*

1. O presente Contrato é celebrado com fulcro nas normas insertas na Lei 8.666/93 e suas alterações, tendo por base as condições estabelecidas no Pregão nº 02/2022 e os termos da proposta apresentada pela Contratada.

CLÁUSULA DÉCIMA QUINTA – *DO FORO*

1. Fica eleito o foro da Seção Judiciária da Justiça Federal de Salvador, capital do Estado da Bahia, para dirimir qualquer dúvida oriunda da execução deste contrato.

2. E, por estarem justas e contratadas, assinam as partes o presente instrumento, em 02 (duas) vias de igual teor e forma, para que produza seus jurídicos e legais efeitos.

Salvador, _____ de _____ de 2022.

TRIBUNAL REGIONAL ELEITORAL DA BAHIA:05967350000145
Assinado de forma digital por TRIBUNAL REGIONAL ELEITORAL DA BAHIA:05967350000145
Dados: 2022.05.10 13:42:56 -03'00'

Raimundo de Campos Vieira
Diretor-Geral do TRE-BA

HERBERT JOSE AZEVEDO:10260365858
Assinado de forma digital por HERBERT JOSE AZEVEDO:10260365858
Dados: 2022.05.10 08:15:00 -03'00'

Herbert José Azevedo
CPF Nº 102.603.658-58
Contratada

FABIO CUNHA:27338922829
Assinado de forma digital por FABIO CUNHA:27338922829
Dados: 2022.05.10 09:06:22 -03'00'

Fábio Cunha
CPF n.º 273.389.228-29
Contratada

ANEXO
TERMO DE REFERÊNCIA

1. OBJETO

1.1 Registro de Preços para Eventual Aquisição de Equipamentos e Programas de Datacenter, conforme especificações constantes do Anexo A deste termo.

2. JUSTIFICATIVA

2.1 Troca de equipamentos críticos em fim de vida útil ou defeituosos, bem como a ampliação do quantitativo existente por conta de novas necessidades, conforme detalhado nos estudos preliminares. Fazem parte dessa iniciativa: Servidores, Unidades de Armazenamento NAS, Unidades de Cópia de Segurança Automatizadas, Programa de Rede Definida por *Software*, Firewall de Aplicações com Balanceador de Carga, Programa de Prospecção de Vulnerabilidades, Certificados Digitais, Sistemas Operacionais e suporte técnico para E-mail Zimbra.

A modalidade de registro de preços é a que mais se adequa às aquisições, visto que todos os itens aqui estão sujeitos a um grau de indeterminação quanto ao quantitativo da eventual aquisição ou quanto ao momento da sua eventual aquisição, considerando-se que ou estão associados a demandas em quantidades variáveis, pois podem requerer ampliações imediatas motivadas por novas demandas de uso pela Administração do Tribunal, ou estão dependentes de conclusão de fases das complexas implantações, traduzindo-se na prática em condições de entregas parceladas ou quantitativo não definido previamente, em consonância ao previsto no art. 3º do Decreto 7892/2013, incisos II e IV:

> *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;*
>
> *IV – quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.*

Para todos os itens a modalidade de licitação indicada é o **pregão eletrônico**. Por questões técnicas como compatibilidade ou de estratégia de implantação visando assegurar uma transição primorosa, adequada a ambientes críticos de produção, houve indicação de marca e modelo para os itens 1, 4, 8, 9, 10, 12 e 13. De maneira sintética, o item 1 expande um quantitativo de equipamentos que só possuem compatibilidade com equipamentos iguais em federação; o item 4 precisa ser compatível com o VMWare VSphere e os sistemas de virtualização dos servidores atuais, que serão expandidos no item 1; o item 8 é serviço de suporte para o produto já adquirido Zimbra; e os itens 9, 10, 12 e 13, conforme detalhado nos estudos preliminares, são licenças de um sistema operacional do qual diversos sistemas em produção no Tribunal são dependentes.

Para todos os itens constam as especificações gerais com a indicação dos modelos de referência. Exceto os itens 9 , 10, 12 e 13, nenhum outro item poderá ter aplicação especificamente do inciso III do artigo 48 da Lei Complementar nº 123/2006 e do inciso IV do artigo 2º do Decreto nº 8.538/2015 devido à necessidade de padronização desses equipamentos, por motivo da implementação da gerência remota centralizada.

O prazo contratual para os itens deverá ser de 60 meses após a assinatura, refletindo o tempo de vigência do suporte técnico. Para os itens 7, 8, 9, 10, 12 e 13, o termo de contrato pode ser substituído por Nota de Empenho. A modalidade de licitação sugerida para este registro de preços é o **pregão eletrônico**, com **preço por item**.

2.1.1. Relação Demanda Prevista e Quantidade a Ser Contratada.

ITEM	DESCRIÇÃO	QUANTIDADE
1	Nó de Hiperconvergência HPE Simplivity Extra-Large. As especificações detalhadas constam no Anexo A deste Termo de Referência.	05 unidades
2	Servidor de Rede. As especificações detalhadas constam no Anexo A deste Termo de Referência.	03 unidades
3	Unidade de Armazenamento NAS. As especificações detalhadas constam no Anexo A deste Termo de Referência.	03 unidades
4	VMWare Network Virtualization and Security Platform Advanced Edition (VMware NSX). As especificações detalhadas constam no Anexo A deste Termo de Referência.	20 unidades
5	Appliance Virtual de Balanceamento de Carga com Firewall de Aplicações. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
6	Programa de Prospecção de Vulnerabilidades em Computadores. As especificações detalhadas constam no Anexo A deste Termo de Referência.	01 unidade
7	Certificados Digitais A1 SSL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	100 unidades
8	Assinatura de Suporte técnico e atualizações para 2000 unidades de Zimbra Network Edition Standard e 250 unidades de Zimbra Network Edition Professional. As especificações detalhadas constam no Anexo A deste Termo de Referência.	01 unidade
9	Licença de Windows Server Datacenter 2019. As especificações detalhadas constam no Anexo A deste Termo de Referência.	7 unidades

ITEM	DESCRIÇÃO	QUANTIDADE
10	Windows Server Datacenter 2019 CAL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	403 unidades
11	Unidade de cópia de segurança automatizada. As especificações detalhadas constam no Anexo A deste Termo de Referência.	02 unidades
12	Licença de Windows Server Datacenter 2019. As especificações detalhadas constam no Anexo A deste Termo de Referência.	93 unidades
13	Windows Server Datacenter 2019 CAL. As especificações detalhadas constam no Anexo A deste Termo de Referência.	1597 unidades

3. LOCAL E PRAZO DE ENTREGA

3.1 A Contratada deverá entregar o material na SEGEP localizada no Edifício-Sede do Tribunal Regional Eleitoral da Bahia (TRE-BA), sito na 1ª Avenida do Centro Administrativo da Bahia, nº 150, Salvador – Bahia, ou, ainda, no Centro de Apoio Técnico – CAT, localizado no Loteamento Porto Seco Pirajá, Quadra A, Lote 16/17, Rua A, Via Marginal da BR 324, Salvador-Ba, conforme opção da Administração a ser informada quando do agendamento da entrega.

3.2 Horários de entrega: 13h às 18h, de segunda à quinta-feira, e 08h às 12h, às sextas-feiras.

3.3 A Contratada deverá, obrigatoriamente, consultar a SEGEP, através dos telefones (71 - 3373-7077 ou 71 - 3373-7357), ou através do e-mail segep@tre-ba.jus.br, para fazer o agendamento da entrega.

3.4 O prazo para a entrega do material solicitado será de 30 dias, contados do recebimento, pela Contratada, do "Pedido de Fornecimento". O Pedido de Fornecimento será emitido pela Fiscalização do Contrato, no prazo máximo de 5 dias, contados da data do recebimento da via contratual/nota de empenho pela Contratada.

3.5 Correrão por conta da Contratada quaisquer providências relativas à descarga do material, incluindo-se aí a necessária mão de obra.

3.6 Em caso de paralisação das atividades dos setores responsáveis pelo recebimento dos bens durante o Recesso Forense (entre 20 de dezembro e 6 de janeiro do ano subsequente), haverá a suspensão dos prazos de entrega em favor da Contratada. Neste caso, a empresa será previamente notificada pela Fiscalização do Contrato.

3.7 Os *softwares* deverão ser entregues suas chaves eletrônicas por e-mail seinfra@tre-ba.jus.br, no prazo máximo de 05 dias úteis, a partir do recebimento do "Pedido de Fornecimento".

4. RECEBIMENTO

4.1 O recebimento ocorrerá em duas etapas:

a) **Recebimento provisório**: o material será recebido provisoriamente no momento da entrega, para efeito de posterior verificação de sua conformidade com as especificações constantes do Edital e da proposta, ficando, nesta ocasião, suspensa a fluência do prazo de entrega inicialmente fixado.

b) **Recebimento definitivo**: no prazo de 05 dias após o recebimento provisório, a Fiscalização do Contrato avaliará as características do material que, estando em conformidade com as especificações exigidas, será recebido definitivamente.

4.2 A Contratada garantirá a qualidade do material fornecido, obrigando-se a substituir aquele que apresentar vícios ou incorreções resultantes da fabricação ou de sua correta utilização que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor.

4.3 Em caso de irregularidades apuradas no momento da entrega, o material poderá ser recusado de pronto, mediante termo correspondente, ficando dispensado o recebimento provisório, e fazendo-se disso imediata comunicação escrita ao fornecedor.

4.4 Se após o recebimento provisório, constatar-se que o fornecimento foi efetuado em desacordo com o pactuado ou foi entregue quantitativo inferior ao solicitado, a Fiscalização do Contrato notificará por escrito a Contratada para substituir, às suas expensas, o material recusado ou complementar o material faltante, no prazo que lhe restar daquele indicado para entrega.

4.5 Se a Contratada não substituir ou complementar o material entregue em desconformidade com as condições exigidas no edital, o fiscal do contrato glosará a nota fiscal, no valor do material não entregue ou recusado, e a encaminhará para pagamento, acompanhada de relatório circunstanciado, informando, ainda, o valor a ser retido cautelarmente, para fazer face a eventual aplicação de multa.

4.6 Caso a Contratada não retire, no prazo de 90 dias, a contar do recebimento da notificação, o material recusado, ficará caracterizado o seu abandono, nos termos do disposto no artigo 1.275, Inciso III, do Código Civil, podendo a Contratante incorporá-lo ao seu patrimônio, encaminhá-lo a outros órgãos da Administração Pública ou, ainda, doá-lo nos termos do disposto no Decreto nº 9.373/2018.

4.7 A Contratada fará constar da nota fiscal os valores unitários e respectivos valores totais em conformidade com o constante da correspondente nota de empenho/contrato, atentando-se para as inexatidões que poderão decorrer de eventuais arredondamentos.

4.8 Consoante o disposto no artigo 32 da Lei n° 12.305/2010, as embalagens dos materiais devem ser fabricadas com materiais que propiciem a reutilização ou a reciclagem, devendo-se assegurar que sejam restritas em volume e peso às dimensões requeridas à proteção do conteúdo e à comercialização do produto, projetadas de forma a serem reutilizadas de maneira tecnicamente viável e compatível com as exigências aplicáveis ao produto que contêm, ou recicladas, se a reutilização não for possível.

5. GARANTIA DE ADEQUAÇÃO DO PRODUTO

5.1 A Contratada, no ato de entrega dos bens, deverá apresentar o Termo de Garantia.

5.2 A Contratada deverá oferecer garantia, pelo prazo mínimo de 60 meses (ou pelo prazo constante na descrição de cada item), contado a partir do recebimento definitivo.

5.3 Na vigência da garantia, a Contratada obrigar-se-á a reparar, sem ônus para a Contratante (garantia on site), o objeto contratado que apresentar vícios ou incorreções resultantes da fabricação ou de sua correta utilização que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor no prazo máximo de 30 dias úteis, a contar do primeiro dia útil seguinte ao do recebimento, pela Contratada, da comunicação de inconformidade.

5.4 O término do atendimento ocorrerá no dia de conclusão do reparo e da disponibilidade do objeto em perfeito estado de uso nas dependências da Contratante.

5.5 O pedido de substituição ou de reparo do objeto contratado, durante o período de garantia, poderá ser formalizado por telefone, e-mail, fax ou outro meio hábil de comunicação.

5.6 Não sendo o vício sanado no prazo do subitem 5.3, a Contratada será notificada para que substitua o produto por outro novo da mesma espécie, marca e modelo, em perfeitas condições de uso, em no máximo 30 dias, a contar do primeiro dia útil seguinte ao do recebimento da notificação, sob pena de serem-lhe aplicadas as sanções previstas no edital e no contrato.

5.7 A garantia, em todos os casos, engloba a proteção contra vícios, defeitos ou incorreções advindas da fabricação, montagem e desgaste excessivo.

6. OBRIGAÇÕES DA CONTRATADA

6.1 São obrigações da Contratada, além daquelas explícita ou implicitamente contidas no presente termo de referência e na legislação vigente:

a) entregar os bens no prazo, nas especificações e na quantidade constantes neste termo de referência, assim como com as características descritas na proposta;

b) atender às solicitações da Contratante nos prazos estabelecidos neste instrumento;

c) não fornecer quantidade ou modelo diversos do solicitado;

d) substituir os produtos danificados em razão de transporte, descarga ou outra situação que não possa ser imputada à Administração;

e) responder pelos encargos previdenciários, trabalhistas, fiscais e comerciais resultantes da execução do contrato;

f) responder por quaisquer danos pessoais ou materiais causados por seus empregados à Administração e/ou a terceiros na execução deste Contrato;

g) manter, durante a execução do ajuste, todas as condições de habilitação exigidas para a contratação;

h) reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

i) não subcontratar, ceder ou transferir, no todo ou em parte, o objeto do contrato, salvo se autorizado neste termo de referência;

j) prestar garantia de adequação dos produtos (qualidade, segurança, durabilidade e desempenho), em conformidade com as condições estabelecidas neste termo de referência.

7. OBRIGAÇÕES DA CONTRATANTE

7.1 A Contratante obriga-se a:

a) acompanhar e fiscalizar a execução do ajuste, anotando em registro próprio as ocorrências acaso verificadas, determinando o que for necessário à regularização das faltas ou defeitos observados;

b) prestar esclarecimentos que venham a ser solicitados pela Contratada;

c) efetuar os pagamentos nas condições e nos prazos constantes neste termo de referência e no edital;

d) zelar para que, durante a vigência do Contrato, a Contratada cumpra as obrigações assumidas, bem como sejam mantidas as condições de habilitação e qualificação exigidas no processo licitatório;

e) determinar a reparação, a correção, a remoção ou a substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções.

8. INADIMPLEMENTO E PENALIDADES

8.1 A Administração poderá aplicar à licitante vencedora, pelo descumprimento total ou parcial das obrigações assumidas, as sanções previstas na Lei e no Contrato, sendo a multa calculada dentro dos seguintes parâmetros:

a) atrasar injustificadamente a entrega do objeto contratado – **0,5%, sobre o valor do material entregue em atraso, por dia de atraso, até o máximo de 20 dias;**

b) inexecução parcial – **20% sobre o valor do material não entregue;**

c) inexecução total – **20% sobre o valor total contratado;**

d) atrasar, até no máximo **15 dias**, o atendimento para a reparação do vício ou incorreções ou a substituição do produto que apresentou, dentro do prazo de garantia, vícios ou incorreções decorrentes da fabricação ou do seu uso correto que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor – **1% do valor de aquisição do bem, por dia de atraso;**

e) não realizar a reparação do vício ou incorreções ou a substituição do produto que apresentou, dentro do prazo de garantia, vícios ou incorreções decorrentes da fabricação ou do seu uso correto que o tornem impróprio ou inadequado para o consumo a que se destina ou lhe diminuam o valor – **20% do valor de aquisição do material não substituído.**

8.2 Ultrapassado o prazo estabelecido no **subitem 8.1, alínea "a",** a Administração poderá não receber os itens pendentes de entrega.

8.3 A aplicação da penalidade estabelecida no **subitem 8.1, alínea "e"** não afasta a obrigação da devolução do valor pago pela aquisição do bem.

9. MEDIDAS ACAUTELADORAS

9.1 Ocorrendo inadimplemento contratual, a Administração poderá, com base no artigo 45 da Lei nº 9.784/1999 e *artigo 26, § 1º, da Portaria nº 305/2019*, do TRE/BA, reter de forma cautelar, dos pagamentos devidos à Contratada, valor relativo a eventual multa a ser-lhe aplicada.

9.2 Finalizado o processo administrativo de apuração das faltas contratuais cometidas pela Contratada, tendo a Contratante decidido pela penalização, o valor retido cautelarmente será convertido em multa. Não havendo decisão condenatória, o valor será restituído, monetariamente corrigido pelo mesmo índice de reajuste dos pagamentos devidos à Contratada.

10. PAGAMENTO

10.1 Observada a ordem cronológica estabelecida no art. 5º da Lei 8.666/93, o pagamento será efetuado sem qualquer acréscimo financeiro, mediante depósito através de ordem bancária, nos seguintes prazos e condições:

10.1.1 Para valor igual ou inferior a R$ 17.600,00: até o 5º dia útil subsequente à apresentação da nota fiscal;

10.1.2 Para valor superior a R$ 17.600,00: até o 10º dia útil subsequente à apresentação da nota fiscal.

10.2 Condiciona-se o pagamento a:

I – Apresentação da nota fiscal discriminativa da execução do objeto contratado;

II – Declaração da Fiscalização do Contrato de que o fornecimento se deu conforme pactuado.

10.3 A Contratada indicará na nota fiscal o nome do Banco e os números da agência e da conta corrente para efetivação do pagamento.

10.4 A Contratante, observados os princípios do contraditório e da ampla defesa, poderá deduzir, do montante a pagar à Contratada, os valores correspondentes a multas, ressarcimentos ou indenizações por esta devidos.

11. MEIOS DE COMUNICAÇÃO

11.1 As notificações emitidas pela Administração que implicarem abertura de prazo para cumprimento de obrigações, assim como as intimações dos despachos ou decisões que imponham deveres, restrições de direito ou sanções à Contratada, deverão ser feitas pessoalmente, mediante ciência nos autos, ou por meio eletrônico, com confirmação inequívoca do recebimento.

11.1.1 Frustradas as tentativas de comunicação pelos meios acima citados, esta deverá ser realizada por correspondência com aviso de recebimento ou por qualquer outro meio idôneo que assegure a certeza da ciência do interessado, ou ainda, em caso de aplicação de sanção, por edital, no Diário Oficial da União – DOU, quando ignorado, incerto ou inacessível o lugar em que o fornecedor se encontrar.

11.1.2 A comunicação dos atos processuais será dispensada quando o representante da Contratada revelar conhecimento de seu conteúdo, manifestado expressamente por qualquer meio.

12. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – LEI 13709/18

12.1 O TRE-BA e a Contratada se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, atuando da seguinte forma:

12.2 Mediante prévia e fundamentada aprovação do TRE-BA, responsabilizando-se a Contratada por obter o consentimento dos titulares (salvo nos casos em quer opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins;

12.3 Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a Contratada providenciará seu descarte de forma segura.

12.4 A Contratada dará conhecimento formal aos seus empregados das obrigações e condições acordadas neste item, inclusive no tocante à Política de Privacidade do TRE-BA, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

12.5 O eventual acesso, pela Contratada, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio implicará para a mesma e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

12.6 Representante da Contratada manterá contato formal com representante do TRE-BA, no prazo de 24 (vinte e quatro) horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes.

12.7 A critério do TRE-BA, a Contratada poderá ser provocada a preencher um relatório de impacto, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

ANEXO A

Especificações

DO TERMO DE REFERÊNCIA

Os códigos e descrições do CATMAT, constantes do SIASG, citados pelo COMPRASNET podem eventualmente divergir da descrição dos itens licitados quanto a especificações e outras características. Havendo divergência quanto ao código/descrição CATMAT, valem as especificações detalhadas neste Termo de Referência.

ITENS EXCLUSIVOS PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE (com base na Lei Complementar 123/2006): 7, 9 e 10

ITENS ABERTOS A TODAS AS LICITANTES, INCLUSIVE ÀQUELAS ENQUADRADAS COMO MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE (COM BASE NA LEI COMPLEMENTAR 123/2006): 1 A 6, 8, 11, 12 e 13

A.1. ESPECIFICAÇÕES DO ITEM 1 (CATMAT 480089)

ITEM 1 - SERVIDOR HPE SIMPLIVITY PART NUMBER Q8D81A OU SUPERIOR	
1	SERVIDOR HPE SIMPLIVITY PART NUMBER Q8D81A (EXTRA-LARGE) OU SUPERIOR
1.1	Deverá possuir, no mínimo, 768 GB de memória;
1.2	Deverá possuir, no mínimo, 12 discos SSD de 3,84TB.
1.3	O prazo de garantia do fabricante para os equipamentos será de no mínimo 60 (sessenta) meses para reposição de peças, mão de obra e atendimento no on-site, no regime 24 x 7, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados e finais de semana, contemplando ainda direito de atualização de versões, releases e patches dos equipamentos, sistemas operacionais, ferramentas de gerenciamento e demais itens correlacionados aos mesmos;

A.2. ESPECIFICAÇÕES DO ITEM 2 (CATMAT 480089)

ITEM 2 – SERVIDOR DE REDE	
2	SERVIDOR DE REDE
2.1	Deverá ser otimizado para rack

2.2	Deverá possuir 02 (duas) controladoras de rede local (25 GbE);
2.3	Deverá possuir processador escalável com no mínimo 16 (dezesseis) núcleos (cores) de execução de instruções por processador, com as seguintes características:
2.4	Microprocessador que implemente pelo menos o set de instruções similar ou igual aos microprocessadores X86, com suporte a aplicações de 64 (sessenta e quatro) bits;
2.4.1	Entende-se por processador um encapsulamento físico composto por no mínimo 16 (dezesseis) núcleos (cores) de execução de instruções.
2.4.2	Deverá possuir *chipset* do mesmo fabricante do processador ou do fabricante da placa-mãe, sendo especializado para servidores;
2.4.3	Deverá possuir instruções de virtualização e suporte a virtualização de I/O;
2.4.4	Deverá possuir suporte a instruções AES (Advanced Encryption Standard) e SSE4;
2.4.5	Deverá fornecer processador Intel, com tecnologia de semicondutor usada para fabricar um circuito integrado com tamanho máximo de 14 nm (quatorze nanômetros);
2.4.6	O barramento dos canais de memória do processador deverá operar na velocidade mínima de 2933 MHz.
2.4.7	Deverá possuir frequência mínima de 3 GHz.
2.4.7.1	Será aceita frequência inferior à solicitada, caso a nova geração do processador tenha sido lançada com frequência inferior, desde que atendidos os demais requisitos mínimos solicitados.
2.4.8	O processador deverá ter sido lançado a partir de janeiro de 2021.
2.5	Deverá possuir UEFI (Unified Extensible Firmware Interface) ou BIOS (Basic Input Output System), devendo suportar integralmente compatibilidade e interoperabilidade com o servidor a ser fornecido sem qualquer perda de funcionalidade, principalmente quanto ao acesso e controle de funções remotamente com console KVM virtual e diagnóstico.
2.5.1	A BIOS/UEFI do servidor deve possuir (assinatura digital) autenticação criptográfica segundo as especificações NIST SP800-147B.
2.5.2	Deverá possuir firmware atualizável por software com data de fabricação posterior a janeiro/2020;
2.5.3	As atualizações de firmwares, BIOS e drivers devem possuir tecnologia de verificação de integridade (assinatura digital) do fabricante do servidor, de modo a garantir a autenticidade da mesma.
2.6	Deverá possuir módulo de segurança TPM (Trusted Platform Module) 2.0 ou superior;
2.7	Deverá possuir número de slots de expansão compatíveis com dispositivos de I/O, na tecnologia PCIExpress v.3 ou superior;

2.8 Deverá possuir controladora de disco com as seguintes características:
2.8.1 Deverá possuir agrupamento em arranjo do tipo RAID-1 por hardware;
2.8.2 Deverá possuir 01 (um) canal padrão SATA 3 (Serial ATA) ou Serial Attached SCSI (SAS);
2.8.3 Taxa de transferência mínima de 6 Gb/s (seis Gigabits por segundo);
2.8.4 A controladora SAS deverá possuir conexão externa para equipamentos de unidade de cópia automatizada;
2.9 Deverá possuir 02 (duas) unidades SSD (Solid State Drive), com as seguintes características:
2.10 Deverá possuir padrão SATA 3 (Serial ATA) ou Serial Attached SCSI (SAS), de no mínimo 0.5 DWPD para 5 anos, especializados para uso em servidores;
2.11 Deverá possuir capacidade mínima de 240 GB (duzentos e quarenta Gigabytes), cada, configuradas em RAID-1;
2.12 Deverá possuir formato M.2 ou 2.5”;
2.12.1 Será aceita a oferta de unidades SSD (Solid State Drive) NVMe, desde que atendidos aos requisitos mínimos solicitados.
2.13 - Possuir controladora de disco com as seguintes características:
2.13.1 Deverá possuir agrupamento em arranjo do tipo RAID 0, 1, 10 e configuração em modo “pass-through ou JBOD” por hardware;
2.13.2 Deverá possuir 01 (um) canal padrão SATA 3 (Serial ATA) ou Serial Attached SCSI (SAS) com taxa de transferência mínima de 6 Gb/s (seis Gigabits por segundo);
2.13.3 Será aceita a oferta de apenas uma controladora para gerenciar os dois grupos de discos acima especificados, desde que atendidos a todos os requisitos mínimos solicitados.
2.14 Deverá possuir unidades SSD (Solid State Drive), com as seguintes características:
2.14.1 Padrão SATA 3 (Serial ATA) ou Serial Attached SCSI (SAS), de no mínimo 3 DWPD para 5 anos, especializados para uso em servidores;
2.14.2 Deverá fornecer doze unidades SSD e capacidade mínima de 1,92 terabytes, cada ou espaço total mínimo de 24 terabytes;
2.15 deverá possuir índice SPECint_rate2017 (baseline) auditado de no mínimo 170 op/s (cento e setenta operações por segundo) para o equipamento fornecido;
2.15.1 Caso o equipamento não tenha sido auditado, deverá ser informado um cálculo estimado, com estimativa de SPECint_rate2017 (baseline) tenha sido obtido a partir de um equipamento auditado do mesmo fabricante dos servidores, com a mesma quantidade de processadores, cores por processador, da mesma família/geração dos processadores fornecidos e mesma frequência de

barramento de sistema. Este índice deverá ser calculado através da expressão abaixo com base em um índice auditado pelo Standard Performance Evaluation Corporation (SPEC) de um equipamento do mesmo fabricante. Índice Estimado = A * B / C, onde: • A = Frequência de clock (em GHz) fornecida para cada processador; • B = Resultado em SPECint_rate2017 (baseline) auditado pela SPEC; • C = Frequência de clock (em GHz) de cada processador utilizado no servidor auditado pela SPEC.
2.15.2 O índice SPECint_rate2017 (baseline) utilizado como referência será validado junto ao site Internet www.spec.org – Standard Performance Evaluation Corporation;
2.15.3 Não serão aceitos resultados obtidos com a utilização de servidores em cluster, bem como estimativas em resultados inferiores ao mínimo especificado no contrato;
2.16 Deverá possuir memória principal DDR4 RDIMM (Registered DIMM) ou LRDIMM (Load Reduced DIMM) com no mínimo, 2933 MT/s;
2.16.1 Deverá possuir capacidade de detecção e correção de erros (ECC) ou correção avançada de erros (Advanced ECC ou SDDC);
2.16.2 Deverá possuir tecnologia de banco de memória reserva ou tecnologia equivalente;
2.16.3 Os canais de memória deverão ter módulos de memória, de mesma capacidade e tipo;
2.16.4 Cada processador deve ter no mínimo 06 (seis) canais ocupados.
2.17 Deverá possuir pelo menos 02 (dois) adaptadores de rede local, PCI-Express v.3 x8 ou superior, sendo possível a oferta de placas on-board e off-board, com as seguintes características:
2.17.1 Padrão IEEE 802.3by e suporte a PXE ou similar;
2.17.2 Suporte a conexões com transceivers 25 GbE SFP28/10 GbE SFP+ com conectores LC;
2.17.3 Configuração por software;
2.17.4 Leds externos de monitoração e diagnósticos;
2.17.5 Gerenciável;
2.17.6 Operar em modo full-duplex;
2.17.7 Deverá permitir implementação de balanceamento de carga;
2.17.8 Possuir suporte a TCP/IP offload Engine (TOE) ou I/O Acceleration Technology (I/OAT) ou tecnologia equivalente que permita a redução do uso da CPU para processamento de pacotes de dados;
2.17.8.1 Caso o equipamento fornecido não disponha de tecnologia embarcada ou área específica para

	armazenamento de todos os drivers necessários para sua correta instalação e suas respectivas interfaces, deverá ser fornecido o endereço do Site oficial Internet do fabricante para download dos drivers;
2.17.9	Não serão aceitas placas de rede em slots inferiores a PCI-Express v.3 x8;
2.17.10	Deverá possuir pelo menos 02 (duas) portas no conjunto dos dois adaptadores solicitados;
2.17.11	Esse adaptador não será utilizado para o gerenciamento do Baseboard Management Controller - BMC.
2.17.12	O prazo de garantia do fabricante para os equipamentos será de no mínimo 60 (sessenta) meses para reposição de peças, mão de obra e atendimento no on-site, no regime 24 x 7, 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, incluindo feriados e finais de semana, contemplando ainda direito de atualização de versões, releases e patches dos equipamentos, sistemas operacionais, ferramentas de gerenciamento e demais i**tens correlacionados aos mesmos;**

A.3. ESPECIFICAÇÕES DO ITEM 3 (CATMAT 451838)

ITEM 3 – UNIDADE DE ARMAZENAMENTO NAS	
3	Armazenamento nativo em disco de, no mínimo, 36 TB úteis para dados, instalados e licenciados, descontadas todas as perdas com redundâncias (RAID) e ganhos com compactação e/ou desduplicação;
3.1	Deverá conter discos com interfaces SAS, SATA (Serial ATA) ou NL-SAS (Near Line SAS) com rotação mínima de 7.2K RPM (sete mil de duzentas rotações por minuto), configurados em RAID 6;
3.2	Deverá acompanhar todos os cabos, acessórios e licenciamento, necessários para integração como o modulo central garantindo assim o perfeito funcionamento da solução. Garantia e suporte do fabricante;
3.3	O prazo de garantia do fabricante para os equipamentos será de no mínimo 60 (sessenta) meses para reposição de peças, mão de obra e atendimento no on-site, no regime 24 x 7, 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, incluindo feriados e finais de semana, contemplando ainda direito de atualização de versões, releases e patches dos equipamentos, sistemas operacionais, ferramentas de gerenciamento e demais itens correlacionados aos mesmos;
3.4	O serviço de suporte técnico para os equipamentos, deverá ser prestado pelo fabricante em regime 24 x 7, 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, incluindo feriados e finais de semana, com tempo de solução máximo de até 6h (seis) horas a partir da abertura do chamado técnico para falhas de hardware;

ITEM 3 – UNIDADE DE ARMAZENAMENTO NAS	
3.5	Todos os componentes dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a sua política de garantia, não sendo permitida a integração de itens de terceiros que possam acarretar perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada;
3.6	A empresa fabricante do equipamento deverá prover assistência técnica on-site na sede da contratante;
3.7	A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos;
3.8	O fabricante do equipamento deverá possuir um sistema atendimento de suporte técnico via Chat, através da Internet;
3.9	O fabricante deverá durante todo período da garantia do equipamento, manter em seu site todos os drivers para os sistemas operacionais suportados e prover todas as atualizações e correções de bug para drivers, softwares e firmware que porventura sejam necessários ao respectivo equipamento de forma proativa;
3.10	Durante todo período de garantia em intervalos máximos de 180 (cento e oitenta) dias, deverão ser enviados pelo fabricante a contratante relatórios contendo a análise de saúde da solução, seguidos das recomendações para aplicação de patchs de correção ou upgrades de fimware, bios que porventura sejam necessários de acordo com o sistema operacional instalado no equipamento de forma a garantir que os equipamentos e softwares, estejam sempre dentro das matrizes de suporte do fabricante e de acordo com as melhores práticas do mesmo. Esse procedimento visa, evitar problemas no processo de atendimento técnico e intervenções não programadas como ainda minimizar possíveis riscos de falhas, paradas ou inatividade dos sistemas alocados nesses equipamentos;
3.11	Deverão ser informados na proposta todos os part numbers de equipamento, software e serviços que compõem as soluções ofertadas. A omissão dessas informações acarretará a desclassificação da proposta. O modelo ofertado deve estar em linha de produção, na data de entrega da proposta;
3.12	Deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de declaração expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados;
3.13	Deverá haver comprovação de que serviços de garantia ofertados na proposta do fabricante/revendedor cobrem as condições exigidas de garantia e suporte e que caso

ITEM 3 – UNIDADE DE ARMAZENAMENTO NAS	
	eventualmente a assistência técnica autorizada local esteja impedida de realizar atendimentos, os mesmos serão realizados por outra autorizada (indicada pelo fabricante) ou pelo próprio fabricante sem ônus adicional para a contratante. Essa comprovação deverá ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogo;
3.14	Deverá ser otimizado para instalação em Rack;
3.15	Deverá possuir, no mínimo, 40 TB de HDs enterprise instalados;
3.16	Deverá possuir capacidade de expansão até 48 TB de HD;
3.17	Deverá possuir processador de, no mínimo, Intel 1,9 GHz e seis núcleos;
3.18	Deverá possuir, no mínimo, 24 baias (sockets) de memória preenchidas com, no mínimo uma memória de 16 GB ou mais;
3.19	Deverá possuir baias de disco Hot-swappable;
3.20	Deverá possuir pelo menos 4 interfaces de rede Gigabit Ethernet RJ45 com recurso de Trunk;
3.21	Deverá possuir pelo menos 2 interfaces USB 3.0;
3.22	Deverá possuir uma interface VGA;
3.23	Deverá possuir capacidade para RAID 0,1,5,6,10;
3.24	Deverá vir acompanhado de software de administração;
3.25	Deverá possuir administração via web, terminal e terminal remoto por ssh;
3.26	Deverá possuir permissões e quotas para usuários e grupos de usuários;
3.27	Deverá suportar protocolos: CIFS/SMB, NFS, FTP, FTPS, SFTP, TFTP, HTTP(S), SSH, iSCSI e SNMP;
3.28	Deverá possuir capacidade de compartilhamento de arquivos com Windows, Mac, Linux/UNIX;
3.29	Deverá possuir alarme e indicação de falha no disco;
3.30	Deverá utilizar Windows Server IoT 2019;
3.31	Garantia de pelo menos 60 meses on-site.

A.4. ESPECIFICAÇÕES DO ITEM 4 (CATSER 27472)

ITEM 4 – SOFTWARE DE REDE DEFINIDA POR SOFTWARE	
4	VMWARE NSX ADVANCED EDITION
4.1	Licenciamento VMware Network Virtualization and Security Platform Advanced edition - NSX por

ITEM 4 – SOFTWARE DE REDE DEFINIDA POR SOFTWARE	
	processador, com direito de atualização de versão;
4.2	Deverá possuir suporte técnico do fabricante pelo período de 60 meses;

A.5. ESPECIFICAÇÕES DO ITEM 5 (CATSER 27472)

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5	**SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES**
5.1	**GERAL**
5.1.1	**Suportar e garantir a instalação em ambiente de alta disponibilidade;**
5.1.2	**A solução ofertada deva trabalhar simultaneamente em diversos modos de operação: Passivo, Ativo, Proxy reverso e Proxy transparente**
5.1.3	**Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo;**
5.1.4	**Fornecer uma solução que opere no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;**
5.1.5	**Assegurar que a operação da solução de 2 ou mais equipamentos, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;**
5.1.6	**Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;**
5.1.7	**A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes**
5.1.8	**O equipamento deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda antes de qualquer equipamento de segurança ;**
5.1.9	**Fornecer recurso de agregação de portas baseado no protocolo LACP**
5.1.10	**Deve possuir suporte a LACP em modo passivo e ativo**
5.1.11	**Fornecer recurso para suportar até 32 portas em um mesmo conjunto agregado;**
5.1.12	**Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s)**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.1.13	**Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;**
5.1.14	**Possuir suporte a IPv6;**
5.1.15	**A solução deve suportar múltiplas tabelas de rotas independentes;**
5.1.16	**O equipamento, quando habilitado para mais de uma função (SLB, GSLB, Aceleração Web, etc), deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade;**
5.1.17	**Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração Web, etc.**
5.1.18	**A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;**
5.1.19	**Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.**
5.1.20	**Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).**
5.1.21	**Gerenciamento da Solução**
5.1.22	**Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;**
5.1.23	**Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);**
5.1.24	**Permitir acesso in-band via SSH;**
5.1.25	**Manter internamente múltiplos arquivos de configurações do sistema;**
5.1.26	**Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;**
5.1.27	**Possuir auto-complementação de comandos na CLI;**
5.1.28	**Possuir ajuda contextual;**
5.1.29	**Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;**
5.1.30	**Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;**
5.1.31	**Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	RADIUS, LDAP e TACACS+ deverão ser suportados;
5.1.32	**Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;**
5.1.33	**A solução deve permitir a integração com bases externas de usuários e grupos, para autenticação e autorização de usuários e grupos administradores da solução, baseado em estrutura de diretório MS Active Directory e LDAP. Portanto deve permitir a associação de diversos grupos de usuários distintos dentro da base externa com distintos níveis de permissão de acordo com o perfil de cada usuário.**
5.1.34	**Possuir Interface Gráfica via Web;**
5.1.35	**A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;**
5.1.36	**A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;**
5.1.37	**Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);**
5.1.38	**Suportar a rollback de configuração e imagem;**
5.1.39	**Permitir integração com a plataforma HP OpenView;**
5.1.40	**Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;**
5.1.41	**Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;**
5.1.42	**Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;**
5.1.43	**A interface Gráfica deverá permitir a reinicialização do equipamento;**
5.1.44	**Reinicialização do equipamento por comando na CLI;**
5.1.45	**Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;**
5.1.46	**Possuir traps SNMP;**
5.1.47	**Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events**
5.1.48	**Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;**
5.1.49	**Implementar Debugging: CLI via console e SSH;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.1.50 Deve possuir suporte a Link Layer Discovery Protocol (LLDP);
5.1.51 Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;
5.1.52 A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
5.1.53 A Solução deve ter suporte a sFlow;
5.2 BALANCEAMENTO
5.2.1 Suportar todas as aplicações comuns de um Switch Layer 7, como:
5.2.1.1 Server Load-Balancing;
5.2.1.2 Firewall Load-Balancing;
5.2.1.3 Proxy Load-Balancing;
5.2.2 Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
5.2.3 A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;
5.2.4 Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;
5.2.5 Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;
5.2.6 A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.
5.2.7 Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.
5.2.8 Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
balanceamento, voltando ao estado original.
5.2.9 Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;
5.2.10 Suportar os seguintes métodos de balanceamento:
5.2.10.1 Round Robin;
5.2.10.2 Least Connections;
5.2.10.3 Weighted Percentage (por peso);
5.2.10.4 Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
5.2.10.5 Weighted Percentage dinâmico (baseado no número de conexões)
5.2.10.6 Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
5.2.11 A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;
5.2.12 Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
5.2.12.1 Por cookie: inserção de um novo cookie na sessão;
5.2.12.2 Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
5.2.12.3 Por endereço IP destino;
5.2.12.4 Por endereço IP origem;
5.2.12.5 Por sessão SSL;
5.2.12.6 Através da análise da URL acessada.;
5.2.12.7 Através da análise de qualquer parâmetro no header HTTP;
5.2.12.8 Através da análise do MS Terminal Services Session (MSRDP)
5.2.12.9 Através da análise do SIP Call ID ou Source IP;
5.2.12.10 Através da análise de qualquer informação da porção de dados (camada 7);
5.2.13 A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
5.2.14 O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
servidores reais:
5.2.14.1 Layer 3 – ICMP;
5.2.14.2 Conexões TCP e UDP pela respectiva porta no servidor;
5.2.15 - Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;
5.2.16 Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);
5.2.17 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
5.2.18 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
5.2.19 Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
5.2.20 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
5.2.21 Realizar Network Address Translation (NAT);
5.2.22 A solução deve suportar NAT de 1-Any. Ou seja, um IP de origem deve sofrer NAT para um range de IPs distintos para evitar a exaustão de 65k portas na conexão entre a solução e o servidor de aplicação.
5.2.23 Realizar Proteção contra Denial of Service (DoS);
5.2.24 Realizar Proteção contra Syn flood;
5.2.25 Realizar Limpeza de cabeçalho HTTP;
5.2.26 A solução deve permitir o controle da resposta ICMP por servidor virtual;
5.2.27 Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;
5.2.28 Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;
5.2.29 Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;
5.2.30 Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.2.31	Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
5.2.32	Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
5.2.33	Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;
5.2.34	Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance;
5.2.35	Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.
5.2.36	Deve possuir a funcionalidade de espelhamento de conexões SSL.
5.2.37	Deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.
5.2.38	Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;
5.2.39	Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
5.2.40	Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
5.2.41	Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
5.2.42	Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
5.2.43	Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.2.43.1 Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
5.2.43.2 Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
5.2.44 A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;
5.2.45 Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPSe SMTPS são enviadas aos servidores sem criptografia;
5.2.46 A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:
5.2.46.1 SSL session cache Timeout
5.2.46.2 Session Ticket;
5.2.46.3 OCSP (Online Certificate Status Protocol) Stapling;
5.2.46.4 Dynamic Record Sizing;
5.2.46.5 ALPN (Application Layer Protocol Negotiation);
5.2.46.6 Perfect Forward Secrecy;
5.2.47 Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;
5.2.48 Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;
5.2.49 Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;
5.2.50 Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
5.2.51 A solução deve suportar Internet Content Adaptation Protocol (ICAP);
5.2.52 Deve ser capaz de realizar DHCP relay;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.2.53 Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
5.2.53.1 Tempo de resposta da aplicação;
5.2.53.2 Latência;
5.2.53.3 Conexões para conjunto de servidores, servidores individuais;
5.2.53.4 Por URL;
5.2.54 A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
5.2.55 Servidores virtuais
5.2.56 Servidores balanceados
5.2.57 URLs
5.2.58 Países de origem, baseados em geolocalização (GEOIP)
5.2.59 Dispositivos de origem do cliente (user agent)
5.2.60 Deve possuir framework unificado para configuração da aplicação
5.2.61 Deve possuir criptografia IPSEC para comunicação entre os balanceadores;
5.2.62 Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;
5.2.63 A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
5.2.64 A Solução deve ter suporte a sFlow;
5.2.65 A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
5.2.66 A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
5.2.67 A solução deve suportar Equal Cost Multipath (ECMP);
5.2.68 A solução deve realizar Bidirectional Forward Detection (BFD);
5.2.69 A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
5.2.70 Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
5.2.71 A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.2.72 A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
5.2.73 A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
5.2.74 A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:
5.2.74.1 Deve ser possível configurar o tamanho máximo da fila;
5.2.74.2 Deve ser possível configurar o tempo máximo de permanência na fila;
5.2.75 A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
5.2.76 A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
5.2.77 A solução deve realizar Controle de Banda baseado em domínio de roteamento;
5.2.78 Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;
5.2.79 Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.
5.2.80 A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
5.2.81 A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;
5.2.82 A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
5.2.83 Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;
5.2.84 Possuir suporte ao protocolo SPDY e HTTP 2.0;
5.2.85 O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.
5.2.86 O equipamento deverá permitir a sincronização das configurações:
5.2.86.1 De forma automática;
5.2.86.2 Manualmente, forçando a sincronização apenas no momento desejado;
5.2.87 Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.2.87.1	Compartilhar a rede de heartbeat com a rede de dados;
5.2.87.2	Utilizar uma rede exclusiva para o heartbeat.
5.2.88	Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
5.2.89	A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.
5.2.90	Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
5.2.91	GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
5.2.92	Deve ser possível tomar as seguintes ações através dessas políticas:
5.2.93	Bloqueio de tráfego
5.2.94	Reescrita e manipulação de URL
5.2.95	Registro de tráfego (log)
5.2.96	Adição de informação no cabeçalho HTTP
5.2.97	Redirecionamento do tráfego para um membro específico
5.2.98	Selecionar uma política específica para Aplicação Web
5.2.99	A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:
5.2.99.1	Endereço IP de origem;
5.2.99.2	Porta TCP ou UDP de origem;
5.2.99.3	Endereço IP de destino;
5.2.99.4	Porta TCP ou UDP de destino;
5.2.99.5	Protocolo de camada 4 (TCP ou UDP);
5.2.99.6	Data e hora da mensagem;
5.2.99.7	URL acessada;
5.2.100	A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
de forma nativa ou no mínimo integrado a uma base Active Directory.
5.2.101 A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.
5.2.102 A solução deve ser capaz de analisar a performance de aplicações web.
5.2.103 A solução deve possuir relatórios das aplicações.
5.2.104 Deve prover métricas de aplicações como: Transações por Segundo;Tempo de latência do cliente e servidor;Throughput de requisição e resposta;Sessões
5.2.105 A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.
5.2.106 As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.
5.2.107 A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.
5.2.108 A geração de informações históricas deverá permitir:
5.2.109 O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;
5.2.110 Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.
5.3 DNS
5.3.1 A solução deve operar em, no mínimo, a seguintes formas:
5.3.1.1 DNS autoritativo;
5.3.1.2 DNS secundário;
5.3.1.3 DNS resolver;
5.3.1.4 DNS cache;
5.3.1.5 Balanceamento de DNS servers;
5.3.1.6 DNSSec;
5.3.2 A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.3.3	Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;
5.3.4	A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
5.3.5	A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;
5.3.6	A solução deve possuir certificação ICSA;
5.3.7	A solução deve possuir proteções contra ataques DNS, no mínimo:
5.3.8	- Inspeção de protocolo;
5.3.9	- Validação de protocolo;
5.3.10	- UDP flood;
5.3.11	- Pacotes mal formados;
5.3.12	- Ataque Teardrop;
5.3.13	- Ataque ICMP;
5.3.14	Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
5.3.15	A solução deve ser capaz de realizar balanceamento dos servidores DNS;
5.3.16	A solução deve ser capaz de realizar filtragem de pacotes;
5.3.17	A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS .
5.3.18	A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.
5.3.19	A solução deve realizar stateful inspection;
5.3.20	A solução deve possuir base de Geolocalização IP;
5.3.21	A solução deve implementar DNS64;
5.3.22	A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
5.3.23	Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.3.24 Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
5.3.25 Deve prover as respostas a queries DNS da própria RAM CACHE
5.3.26 A solução deve ser capaz de realizar IP Anycast;
5.3.27 A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso
5.3.28 A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
5.3.29 A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;
5.3.30 A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;
5.3.31 Deve ser possível ajustar quantos endereços são enviados em uma única resposta;
5.3.32 Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;
5.3.33 Suportar pelo menos os seguintes algoritmos de balanceamento:
5.3.33.1 Round Robin;
5.3.33.2 Global Availability;
5.3.33.3 Ratio;
5.3.33.4 LDNS Persist;
5.3.33.5 Geografia;
5.3.33.6 Disponibilidade da Aplicação;
5.3.33.7 Capacidade do Virtual Server;
5.3.33.8 Least Connections;
5.3.33.9 Pacotes por segundo;
5.3.33.10 Round trip time;
5.3.33.11 Hops;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.3.33.12	**Packet Completion Rate**
5.3.33.13	**QoS definido pelo usuário;**
5.3.33.14	**Kilobytes per Second;**
5.3.34	**Implementar persistência da conexão do usuário entre aplicações ou data centers;**
5.3.35	**A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;**
5.3.36	**A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;**
5.3.37	**A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;**
5.3.38	**A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);**
5.3.39	**Possuir suporte a IPv6 no balanceamento global entre datacenters.**
5.3.40	**Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.**
5.3.41	**Deverá possuir a funcionalidade de resposta rápida a queries DNS. permitindo respostas mais rápidas para zonas que seja autoritativo.**
5.3.42	**A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.**
5.3.43	**A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (GSLB) ou encaminhar requisições de clientes (screening).**
5.3.44	**Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões.**
5.3.45	**A solução deve funcionar pelo menos das seguintes formas:**
5.3.46	**Usar o ECS para tomar decisões de GSLB baseado em topologia (Subnets)**
5.3.47	**Injetar o ECS (proxy requests) para outros servidores DNS**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.3.48	**A solução deve fazer persistencia baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS), o GSLB deve usar a persistêcnia existente para manter o cliente no mesmo Datacenter.**
5.3.49	**Serviço de DNS com Firewall DNS**
5.3.50	**O serviço deverá ser implementado sobre uma infraestrutura de hardware e software dedicada ou em conjunto com equipamento Anti-DDoS. O hardware empregado deverá ser do tipo appliance, específico para operar softwares de DNS Firewall. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional. O serviço deve ter suporte a IPv6, registros AAAA e zonas reversas IPv6.**
5.3.51	**Infraestrutura de hardware e software destinada à função de resolução de nomes DNS de uso exclusivo da CONTRATANTE.**
5.3.52	**O serviço deve ter a habilidade de detectar, monitorar, controlar e mitigar ataques baseados em DNS sem gerar nenhum impacto ao tráfego válido de DNS.**
5.3.53	**A solução deverá ter serviço de resolução de nomes destinado a armazenar, de forma "autoritativa", as zonas do CONTRATANTE e o IP reverso do bloco CIDR do CONTRATANTE.**
5.3.54	**Os equipamentos que atenderão ao serviço deverão ser estruturados de forma redundante, permitindo o failover completo na ocorrência de falhas, suportando, no mínimo, o modo de operação ativo-ativo. Um nó deverá suportar sozinho todos os requisitos de performance solicitados neste projeto.**
5.3.55	**Para o devido dimensionamento do serviço cada equipamento isolado deve possuir desempenho DNS de pelo menos 50.000 QPS (50 mil Queries Per Second – Consultas Por Segundo).**
5.3.56	**O serviço deverá possuir capacidade para resolver consultas para as quais não tem autoridade (ou seja, da zona ".", tipo "hint"), com a finalidade de atender somente às consultas DNS oriundas da rede interna do CONTRATANTE, bem como dos demais Serviços Gerenciados de Segurança e servidores instalados no Data Center.**
5.3.57	**O serviço deve ter, pelo menos, as seguintes características de segurança:**
5.3.58	**Deve permitir o uso de lista negra para bloquear domínios DNS.**
5.3.59	**Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas.**
5.3.60	**Prover uma linha de defesa para bloquear tentativas de acesso a sites maliciosos impedindo a resolução de nomes de domínio que hospedem tais conteúdos maliciosos minimizando**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet).
5.3.61	**Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso. Estes registros devem conter: IP de origem, destino, data e hora do acesso.**
5.3.62	**Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio.**
5.3.63	**A solução deverá suportar mecanismo de "assinaturas", ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento.**
5.3.64	**O serviço deverá permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:**
5.3.65	**Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP.**
5.3.66	**Bloqueio de endereços de origem IPv4 ou IPv6 em consultas realizadas via TCP ou UDP. Esta regra deverá permitir a configuração de endereços de hosts ou de redes.**
5.3.67	**Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado.**
5.3.68	**De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP.**
5.3.69	**Criar "Listas brancas" que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem.**
5.3.70	**O serviço deverá proteger contra os seguintes ataques de DNS:**
5.3.71	**Reflexão.**
5.3.72	**Anomalias de Protocolo.**
5.3.73	**Negação de Serviço.**
5.3.74	**Negação de Serviços Distribuídos.**
5.3.75	**Amplificação.**
5.3.76	**Tunelamento.**
5.3.77	**Reconhecimento.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.3.78	Explorações (Exploit).
5.3.79	Envenenamento do cache.
5.3.80	Excessos (Floods).
5.3.81	O serviço deve permitir que os administradores efetuem busca de endereços de rede, subrede e endereços IP através de filtros.
5.3.82	A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração.
5.3.83	O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup.
5.3.84	O serviço deverá fornecer pelo menos os seguintes relatórios:
5.3.85	Tendência de latência de resposta de DNS.
5.3.86	Nomes de domínios de DNS mais requisitados.
5.3.87	Tendência de uso do cache de DNS.
5.3.88	Top clientes de DNS.
5.3.89	Taxa de consultas de DNS por tipo de registro.
5.3.90	Tendências de respostas de DNS.
5.3.91	Taxa de consultas de DNS diária por servidor.
5.3.92	Pico de consultas diárias de DNS por servidor.
5.3.93	Top DNS NXDOMAIN/No error.
5.3.94	Top SERVFAIL enviados e recebidos.
5.3.95	Top clientes por domínio de DNS.
5.3.96	Nomes de domínios com conteúdo malicioso.
5.3.97	Principais domínios maliciosos.
5.3.98	Principais acessos ao DNS Firewall.
5.3.99	Quantidade de eventos registrados por horário.
5.3.100	Quantidade de eventos por severidade.
5.3.101	Quantidade de eventos por regra.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
5.3.102 Quantidade de eventos por tendência.
5.3.103 Quantidade de eventos por categoria.
5.3.104 Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições.
5.3.105 Deve implementar DNSSEC com suporte a NSEC3 (RFC 5155).
5.4 FIREWALL DE DATA CENTER
5.4.1 A solução deve atuar como stateful firewall;
5.4.2 solução deve atuar como full-proxy;
5.4.3 A solução deve permitir a criação de logs customizados por aplicação;
5.4.4 A solução deve terminar as conexões SSL com a finalidade de inspecioná-las;
5.4.5 A solução deve proteger de ataques DDoS nas camadas de rede e de sessão;
5.4.6 A solução deve possuir linguaguem de programação que garanta a flexibilidade;
5.4.7 A solução deve proteger de ataques DDoS que utilizem SSL
5.4.8 A solução deve permitir a criação de regras com, no mínimo, os seguintes parâmetros:
5.4.9 - Endereço IP destino
5.4.10 - Endereço IP de origem
5.4.11 - Porta de destino
5.4.12 - Porta de origem
5.4.13 - VLAN
5.4.14 - Protocolo
5.4.15 - Ação
5.4.16 - Horário
5.4.17 - Log
5.4.18 A solução deve permitir definir agendamento para ativação da regra;
5.4.19 A solução deve permitir definir, no mínimo, as seguintes ações no tráfego:
5.4.20 - Permitir: os pacotes são aceitos e passam pelo firewall;
5.4.21 - Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	similar a origem do tráfego;
5.4.22	**- Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;**
5.4.23	**Deve ser possível criar regras que sejam aplicadas em diferentes pontos, no mínimo:**
5.4.24	**- Global;**
5.4.25	**- Domínio de Roteamento;**
5.4.26	**- Virtual Server;**
5.4.27	**Deve possuir criptografia IPSEC para comunicação entre os sites.**
5.4.28	**Permitir a configuração de múltiplas contas de usuário local;**
5.4.29	**Fornecer controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;**
5.4.30	**Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de thresholds baseados na baseline da rede ou através de limites de tráfego atingido.**
5.4.31	**Permitir a restauração das configurações de proteções originais;**
5.4.32	**Permitir a configuração em alta disponibilidade;**
5.4.33	**Implementar solução de redundância dos appliances em modo ativo-ativo, de maneira que em caso de falha de um dos appliances, o outro seja capaz de atender a todas as conexões sem downtime e queda de sessões**
5.4.34	**Deve permitir criar lista de exceção de regras (whitelist/blacklist) por endereço IP específico ou faixa de sub-rede**
5.4.35	**O hardware dos appliances deverá possuir capacidade de atender todas as funcionalidades e desempenho solicitados no documento sem exaustão dos recursos de memória e processamento.**
5.4.36	**Todas as licenças de uso permanentes necessárias para possibilitar o seu funcionamento de acordo com as especificações definidas**
5.4.37	**Todos os softwares devem ser entregues com cessão de direito de uso permanente, para usuários ilimitados.**
5.4.38	**Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.4.39	**Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;**
5.4.40	**Bloqueio de pacotes inválidos (incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, Bad IGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN && FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack) e fornecer estatísticas para os pacotes descartados;**
5.4.41	**Bloqueio de ataques em serviços HTTP;**
5.4.42	**Descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período de tempo configurável;**
5.4.43	**Bloqueio de requisições DNS na porta 53 malformadas**
5.4.44	**Limitar o número de consultas DNS por segundo através da configuração de uma taxa (thresholds)**
5.4.45	**Detectar e descartar pacotes HTTP que não atendam aos padrões RFC e, em seguida, barrar os hosts de origem;**
5.4.46	**Executar a atualizações necessárias para prevenção de novos ataques;**
5.4.47	**Mitigar, no mínimo, os seguintes tipos de ataques:**
5.4.48	**ICMP/UDP/TCP FloodS;**
5.4.49	**TCP Flag Abuses;**
5.4.50	**GET/POST FloodS;**
5.4.51	**SYN Floods;**
5.4.52	**UDP Bandwidth Attacks;**
5.4.53	**Smurfing;**
5.4.54	**NTP Reflection Attacks;**
5.4.55	**TCP/UDP Bandwidth Attacks;**
5.4.56	**Fragging Attack;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.4.57	**Slowloris;**
5.4.58	**Connection Attacks;**
5.4.59	**Botnet;**
5.4.60	**Fragmentation attacks;**
5.4.61	**A solução deve possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.**
5.4.62	**A solução deve fazer o rate limiting do volume de logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda.**
5.4.63	**A solução deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS.**
5.4.64	**Deve possuir suporte ao envio de SNMP traps para cada ataque DoS detectado.**
5.5	**WAF**
5.5.1	**A solução deve operar nos modos ativo-ativo e ativo-standby;**
5.5.2	**O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7);**
5.5.3	**Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.**
5.5.4	**Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem ser auto-ajustáveis e adpatativos de acordo com mudanças.**
5.5.5	**A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.**
5.5.6	**A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.**
5.5.7	**O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);**
5.5.8	**Permitir a utilização de um modelo positivo de segurança para proteger contra ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.5.9	**Possuir política de segurança de aplicações web pré-configurada na solução.**
5.5.10	**Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;**
5.5.11	**Permitir a criação de políticas diferenciadas por aplicação.**
5.5.12	**Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;**
5.5.13	**A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;**
5.5.14	**A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect.**
5.5.15	**A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;**
5.5.16	**Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;**
5.6	**GARANTIA DO PRODUTO:**
5.7	**Os produtos devem possuir licenciamento perpétuo, garantia e suporte do fabricante por 60 (sessenta) meses;**
5.8	**A garantia do produto deve iniciar-se conforme descrito nos prazos deste Termo de Referência.**
5.9	**A garantia deve compreender:**
5.10	**A troca do equipamento ou algum de seus componentes em caso de falha, como defeito de fabricação, panes elétricas de peças, entre outros;**
5.11	**Disponibilização de correção de falhas, atualização dos produtos, incluindo vacinas, assinaturas, bases de dados sem ônus adicional para a CONTRATANTE;**
5.12	**Prazos para troca de equipamentos ou componentes:**
5.13	**4 horas para o caso de indisponibilidade total da solução;**
5.14	**72 horas para os demais casos;**
5.15	**Será permitida a troca temporária do equipamento por outro igual ou superior por até 30 dias quando não for possível atender ao requisito do item anterior.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.16	**Se houver substituição em decorrência de assistência técnica, o equipamento, peça ou componente deverá ser homologado pelo fabricante dos equipamentos e, no mínimo, apresentar as mesmas características de desempenho do serviço antes da apresentação do problema;**
5.17	**Caso seja necessário enviar o equipamento, peça ou componente para um centro de assistência técnica fora das dependências da CONTRATANTE, a CONTRATADA deverá desinstalar, embalar, transportar e reinstalar, bem como deverá arcar com todos os custos necessários;**
5.18	**Para a remoção de equipamento, peça e componente será necessária autorização de saída por escrito emitida por servidor da CONTRATANTE, a ser concedida ao funcionário da CONTRATADA, formalmente identificado;**
5.19	**Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo, mas não englobando mudança de hardware:**
5.20	**Patches, fixes, correções, updates e servicepacks;**
5.21	**Novas releases, builds e funcionalidades;**
5.22	**O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito;**
5.23	**O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência da garantia;**
5.24	**A correção de falhas do fabricante deve incluir:**
5.25	**Atualização do sistema (software upgrades);**
5.26	**A correção de falhas do fabricante deve incluir:**
5.27	**Atualização do sistema (software upgrades);**
5.28	**Assistência remota online e por telefone;**
5.29	**Assistência proativa para manutenção planejada;**
5.30	**Acesso à base de conhecimento de problemas e suas resoluções, incluindo, mas não se limitando a download de softwares, ferramentas de licenciamento, guias do produto, notas de lançamento;**
5.31	**Recebimento, por e-mail, alertas de segurança sobre questões relacionadas à ferramenta;**
5.32	**Qualquer ação para atualização deve ser realizada com anuência da CONTRATANTE;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
5.33	**SERVIÇOS DE IMPLANTAÇÃO:**
5.34	**Para todo o produto (hardware ou software) adquirido no escopo deste item, deverá ser fornecido serviço especializado de instalação, customização e configuração da solução contratada no ambiente do TRE-BA. Entende-se por serviço especializado de instalação, customização e configuração a instalação e configuração lógica de todos os softwares envolvidos, de acordo com a necessidade do TRE-BA;**
5.35	**Deverão ser fornecido dois vouchers individuais de Treinamento Oficial do Fabricante para Configuração e Operação do Appliance Virtual de Balanceador de Carga com Firewall de Aplicações e seu Módulo de Entrega de Aplicações (ADC);**
5.36	**A CONTRATADA deverá fornecer o(s) certificado(s) digital(is) SSL necessários para o funcionamento do software.**

A.6. ESPECIFICAÇÕES DO ITEM 6 (CATSER 27472)

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
6	PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.1	A solução deve possuir licenciadas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware);
6.2	A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
6.3	A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
6.4	Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
6.5	A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar ouso de regras com parâmetros específicos para aplicação das mesmas;
6.6	Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
6.7	A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;
6.8	A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
6.9	A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.10 Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as eguintes características:
6.10.1 Por sistema operacional;
6.10.2 Por um determinado software instalado;
6.10.3 Por Ativos impactados por uma determinada vulnerabilidade.4.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability Assessment Language);
6.11 Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
6.12 Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
6.13 A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
6.14 A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
6.15 O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
6.15.1 CVSSv3 Impact Score;
6.16 Idade da Vulnerabilidade;
6.17 Se existe ameaça ou exploit que explore a vulnerabilidade;
6.18 Número de produtos afetados pela vulnerabilidade;
6.19 Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindofeeds de inteligência de ameaças ao vivo;
6.20 Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, aextração de dados para carga no SIEM.
6.21 Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para asvulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
6.22 A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente nosistema operacional;
6.23 A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
6.24 A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
6.25 A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
monitoramento emtempo real;
6.26 A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
6.26.1 Execução de verificação completa do sistema (rede), adequada para qualquer host;
6.26.2 verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
6.26.3 Autenticação de hosts e enumeração de atualizações ausentes;
6.26.4 Execução de varredura simples para descobrir hosts ativos e portas abertas;
6.26.5 Utilização de um scanner para verificar aplicativos da web;
6.26.6 Avaliação de dispositivos móveis;
6.26.7 Auditoria de configuração de serviços em nuvem de terceiros;
6.26.8 Auditoria de configuração dos gerenciadores de dispositivos móveis;
6.26.9 Auditoria de configuração dos dispositivos de rede;
6.26.10Auditoria de configurações do sistema em relação a uma linha de base conhecida;
6.26.11Detecção de desvio de segurança Intel AMT;
6.26.12Verificação de malware nos sistemas Windows e Unix;
6.27 Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;
6.28 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
6.28.1.1 Bancos de dados;
6.28.1.2 Hypervisors (no mímino VMWare ESX/ESXi);
6.28.1.3 Dispositivos móveis;
6.28.1.4 Dispositivos de rede;
6.28.1.5 Endpoints;
6.28.1.6 Aplicações;
6.29 A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
6.30 Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.31 A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
6.32 A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia detodos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo deacordo com as funcionalidades previstas neste Termo de Referência.
6.33 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
6.34 Configuração de segurança e acesso à gerência da solução:
6.34.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
6.34.2 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
6.34.3 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
6.34.4 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
6.34.5 Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;e) Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
6.34.6 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
6.34.7 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;
6.34.8 A empresa contratada não deverá ter acesso a rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premise).
6.35 Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
6.36 Dos Relatórios:
6.37 Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
6.38 A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
6.39 Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
6.40 A solução deve suportar o envio automático de relatórios para destinatários específicos;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
6.41	Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
6.42	Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
6.43	A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
6.44	A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
6.45	A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
6.46	A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
6.47	Hosts verificados sem credenciais;
6.48	Top 100 Vulnerabilidades mais críticas;
6.49	Top 10 Hosts infectados por Malwares;
6.50	Hosts exploráveis por Malwares;
6.51	Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
6.52	Vulnerabilidades críticas e exploráveis;
6.53	Máquinas com vulnerabilidades que podem ser exploradas;
6.54	A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
6.55	A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.
6.56	O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante aque tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
6.57	A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
6.58	A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
6.59	Deve permitir a configuração de vários painéis e widgets;
6.60	Deve ser capaz de medir e reportar ameaças;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
6.61	Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
6.62	A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menoshosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
6.63	A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiõese gerenciar todos por uma console central;
6.64	A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e MacOS, para o monitoramento contínuo de configurações e vulnerabilidades;
6.65	A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
6.66	A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
6.67	A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras nãopodem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
6.68	No caso em que uma atividade de varredura seja interrompida por invadir o período não permitido, o mesmo deve sercapaz de ser reiniciado de onde parou;
6.69	A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
6.70	A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindocontas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;
6.71	A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrãoaté acesso de sistema ou administrativo;
6.72	A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais
6.73	A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o períodode garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final doperíodo que foram aplicadas ou instaladas na solução;
6.74	A aquisição dos itens poderá ser composta em relação ao tempo e a quantidade de ativos e aplicações Web:
6.75	A solução deve estar licenciadas e inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades,avaliação de configuração e conformidade (baseline e compliance),

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
	indícios e padrões de códigos maliciosos conhecidos(malware);
6.76	A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;
6.77	A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;
6.78	Deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);
6.79	A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar ouso de regras com parâmetros específicos para aplicação das mesmas;
6.80	Deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score;
6.81	A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança,sistema e conformidade, bem como hierarquias e prioridades;
6.82	A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;
6.83	A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;
6.84	Deve possuir um sistema de busca de informações de um determinado ativo com no mínimo as seguintes características:
6.85	Por sistema operacional;
6.86	Por um determinado software instalado;
6.87	Por Ativos impactados por uma determinada vulnerabilidade.4.1.11. A solução deve possuir suporte para a adição de detecções personalizadas usando oOVAL Open Vulnerability Assessment Language);
6.88	Deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;
6.89	Possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;
6.90	A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;
6.91	A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;
6.92	O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:
6.93	CVSSv3 Impact Score;
6.94	Idade da Vulnerabilidade;
6.95	Se existe ameaça ou exploit que explore a vulnerabilidade;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
6.96	Número de produtos afetados pela vulnerabilidade;
6.97	Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindofeeds de inteligência de ameaças ao vivo;
6.98	4Deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, aextração de dados para carga no SIEM.
6.99	Deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;
6.100	A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente nosistema operacional;
6.101	A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;
6.102	A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;
6.103	A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;
6.104	A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:
6.104.1	Execução de verificação completa do sistema (rede), adequada para qualquer host;
6.104.2	verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;
6.104.3	Autenticação de hosts e enumeração de atualizações ausentes;
6.104.4	Execução de varredura simples para descobrir hosts ativos e portas abertas;
6.104.5	Utilização de um scanner para verificar aplicativos da web;
6.104.6	Avaliação de dispositivos móveisg. Auditoria de configuração de serviços em nuvem de terceiros;
6.104.7	Auditoria de configuração dos gerenciadores de dispositivos móveis;
6.104.8	Auditoria de configuração dos dispositivos de rede;
6.104.9	Auditoria de configurações do sistema em relação a uma linha de base conhecida;
6.104.10	Detecção de desvio de segurança Intel AMT;
6.104.11	Verificação de malware nos sistemas Windows e Unix;
6.105	Deve ser possível determinar em tempo real quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.106 A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:
6.106.1 Bancos de dados;
6.106.2 Hypervisors (no mímino VMWare ESX/ESXi);
6.106.3 Dispositivos móveis;
6.106.4 Dispositivos de rede;
6.106.5 Endpoints;
6.106.6 Aplicações;
6.107 A solução deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede;
6.108 Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;
6.109 A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBMQRadar, Microfocus ArcSight e Splunk.
6.110 A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas neste Termo de Referência.
6.111 A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.
6.112 Configuração de segurança e acesso à gerência da solução:
6.112.1 Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;
6.112.2 Os dados em trânsito devem usar ao menos o algoritmo TLS 1.2 de chave 2048 bits;
6.112.3 Os dados em trânsito devem ser criptografados ao menos com o algoritmo AES-128 bits;
6.112.4 Os algoritmos de hash devem usar ao menos o algoritmo SHA-256;
6.112.5 Será aceito como comprovação critérios de criptografia publicação em site do fabricante ou declaração do próprio fabricante;
6.112.6 Os dados armazenados devem ser criptografados ao menos com o algoritmo AES-256 bits;
6.112.7 Somente servidores da Contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;
6.112.8 A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.112.9A empresa contratada não deverá ter acesso a rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premise).
6.113 Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.
6.114 Dos Relatórios:
6.115 Deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;
6.116 A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo inclusive a seleção de todos os ativos existentes;
6.117 Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);
6.118 A solução deve suportar o envio automático de relatórios para destinatários específicos;
6.119 Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;
6.120 Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;
6.121 A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;
6.122 A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;
6.123 A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;
6.124 A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:
6.125 Hosts verificados sem credenciais;
6.126 Top 100 Vulnerabilidades mais críticas;
6.127 Top 10 Hosts infectados por Malwares;
6.128 Hosts exploráveis por Malwares;
6.129 Total de vulnerabilidades que podem ser exploradas pelo Metasploit;
6.130 Vulnerabilidades críticas e exploráveis;
6.131 Máquinas com vulnerabilidades que podem ser exploradas;
6.132 A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;
6.133 A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES	
	limites de endereços IPs.
6.134	O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
6.135	A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades, de acordo com a quantidade de endereços IP licenciados;
6.136	A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);
6.137	Deve permitir a configuração de vários painéis e widgets;
6.138	Deve ser capaz de medir e reportar ameaças;
6.139	Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;
6.140	A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;
6.141	A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;
6.142	A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e MacOS, para o monitoramento contínuo de configurações e vulnerabilidades;
6.143	A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
6.144	A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.
6.145	A plataforma de software deve incluir a capacidade de programar períodos de tempo e data em que varreduras não podem ser executadas, como por exemplo em determinados dias do mês ou determinados horários do dia;
6.146	No caso em que uma atividade de varredura seja interrompida por invadir o período não permitido, deve ser capaz de ser reiniciado de onde parou;
6.147	A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;
6.148	A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

ITEM 6 – PROGRAMA DE PROSPECÇÃO DE VULNERABILIDADES
6.149 A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrãoaté acesso de sistema ou administrativo;
6.150 A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais
6.151 A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

A.7. ESPECIFICAÇÕES DO ITEM 7 (CATSER 27472)

ITEM 7 – CERTIFICADOS DIGITAIS A1 SSL
7 CERTIFICADOS DIGITAIS A1 SSL
7.1 Certificado digital SSL A1 para Servidor-Web, de Cadeia Internacional, com validade de 1 (um) ano, que possibilite identificação nativa nos navegadores Mozilla Firefox, Chrome, Edge, Internet Explorer e Safari;
7.2 A instalação do código do certificado deverá ser realizada tanto em servidores Linux quanto Windows;
7.3 O certificado deverá garantir identificação segura e inequívoca dos sistemas a qualquer tempo;
7.4 A validade dos certificados deverá ser de 1 (um) ano e deverão ser emitidos para instalação em até 3 (três) dias úteis após o recebimento da nota de empenho ou da assinatura do contrato.

A.8. ESPECIFICAÇÕES DO ITEM 8 (CATSER 27472)

ITEM 8 –SUPORTE TÉCNICO PARA ZIMBRA NETWORK EDITION
8 SUPORTE TÉCNICO PARA ZIMBRA NETWORK EDITION
8.1 Suporte técnico por 60 meses para 2000 unidades de software Zimbra Collaboration Network Edition Standard
8.2 Suporte técnico por 60 meses para 250 unidades de software Zimbra Collaboration Network Edition Professional

A.9. ESPECIFICAÇÕES DO ITEM 9* (CATSER 27472)

***Cota reservada – item relacionado ao item 12 (cota principal) para fins do disposto no § 3º do art. 8º do Decreto nº 8.538/2015".**

ITEM 9 – LICENÇA DE MICROSOFT WINDOWS SERVER DATACENTER	
9	**MICROSOFT WINDOWS SERVER DATACENTER**
9.1	**Licenciamento Microsoft Windows Server Datacenter por pacotes com 2 cores;**
9.2	**Deve ser fornecida licença da versão mais atual do software, com possibilidade de downgrade para a versão 2019**
9.3	**O suporte técnico deverá ser balcão, de 12 meses.**

A.10. ESPECIFICAÇÕES DO ITEM 10* (CATSER 27472)

Cota reservada – item relacionado ao item 13 (cota principal) para fins do disposto no § 3º do art. 8º do Decreto nº 8.538/2015".

ITEM 10 – LICENÇA CAL DE MICROSOFT WINDOWS SERVER	
10	**MICROSOFT WINDOWS SERVER CAL**
10.1	**Licenciamento CAL do Microsoft Windows Server por dispositivo;**
10.2	**Deve ser fornecida licença da versão mais atual do software, com possibilidade de downgrade para a versão 2019**
10.3	**O suporte técnico deverá ser balcão, de 12 meses.**

A.11. ESPECIFICAÇÕES DO ITEM 11 (CATSER 27758)

ITEM 11 – UNIDADE DE CÓPIA DE SEGURANÇA AUTOMATIZADA	
11	**UNIDADE DE CÓPIA DE SEGURANÇA AUTOMATIZADA**
11.1	**Deverá possuir mecanismo robotizado que permita automação completa da movimentação dos cartuchos internamente com um mínimo de duas controladoras SAS redundantes e hot swap (que suportam troca durante o uso sem interrupção de funcionamento), provendo redundância de caminhos (1 para cada drive) em substituição a exigência de ser hot swap;**
11.2	**Deverá possuir LEDs frontais e/ou display indicador do status de funcionamento;**

ITEM 11 – UNIDADE DE CÓPIA DE SEGURANÇA AUTOMATIZADA	
11.3	Deverá possuir leitor de código de barras integrado, com o objetivo de ler as etiquetas dos cartuchos;
11.4	Deverá possuir uma quantidade mínima de 32 (trinta e dois) slots LTO, disponíveis e prontos para uso (incluindo quaisquer opcionais de ativação que se façam necessários e não considerando cartuchos dentro dos drives) suportando a expansão mínima até 270 (duzentos e setenta) slots para cartuchos LTO, através da aquisição de módulos adicionais ou através do simples licenciamento de slots presentes no equipamento ofertado;
11.5	Possuir compartimento para inserção/retirada de pelo menos 05 (cinco) cartuchos sem realizar inventário global (I/O Slot ou Mail Slot), garantindo assim a operação contínua da biblioteca durante esse processo;
11.6	Deve ser capaz de funcionar em modo de acesso Sequencial e Aleatório a cartuchos;
11.7	Considerar mídias etiquetadas para acesso Aleatório;
11.8	Deve suportar o particionamento do equipamento em até 20 (vinte) unidades lógicas, permitindo assim que cada unidade lógica criada (partição) seja apresentada e operada como uma unidade independente;
11.9	O equipamento deverá suportar criptografia dos dados por hardware, através de licenciamento opcional;
11.10	Possuir a capacidade para utilização de pelo menos 03 (três) drives LTO (Linear Tape Open) geração Ultrium 6/7/8, ou simplesmente LTO-6/LTO-7/LTO-8, suportando instalação futura de 21 (vinte e um) drives adicionais por meio de módulos adicionais ou através da simples inclusão de unidades adicionais no gabinete padrão do equipamento ofertado;
11.11	A biblioteca deverá ser fornecida com dois drives SAS LTO-8 instalados;
11.12	Deverá vir acompanhada de 50 unidades de fita ULTRIUM LTO-8, do próprio fabricante se houver;
11.13	Para efeito de compatibilidade e reaproveitamento, a biblioteca deverá ser integralmente compatível com os drives fibre-channel LTO-6 da tape library HPE MSL-6480 de propriedade e atualmente em uso por este Tribunal, ou seja, deve ser capaz de receber fisicamente o drive e ser possível sua plena utilização;
11.14	Possuir taxa de transferência individual de 300 MB/s (trezentos megabytes por segundo) em cada drive LTO-7 e LTO-8 ofertados. Considerar taxa nominal máxima nativa (sem compressão);
11.15	Oferecer interfaces SAS de forma nativa para os drives ofertados na Tape Library;
11.16	O gerenciamento do equipamento ofertado deverá ser através de rede ethernet utilizando

ITEM 11 – UNIDADE DE CÓPIA DE SEGURANÇA AUTOMATIZADA	
	porta RJ45;
11.17	**Oferecer gerenciamento remoto através de interface web, incluindo as principais funções de operação e monitoração do sistema;**
11.18	**Deve possuir um mínimo de 02 (duas) fontes com funcionamento redundante;**
11.19	**Deve trabalhar com tensão elétrica nominal de 100-240 V (cem a duzentos e quarenta volts) AC a 60 Hz (sessenta hertz);**
11.20	**Devem ser fornecidos cabos, terminadores e demais acessórios para viabilizar a instalação e o funcionamento da Tape Library;**
11.21	**O gabinete deve seguir padrão industrial para racks de 19'' (dezenove polegadas), incluindo porcas, trilhos, parafusos e demais acessórios necessários para sua instalação em rack;**
11.22	**Deverá possuir garantia do fabricante mínima de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento no Onsite, no regime 24 x 7, 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, incluindo feriados e finais de semana;**
11.23	**Deverá possuir Tempo de solução máximo de até 6h (seis) horas a partir da abertura do chamado técnico para falhas de hardware;**
11.24	**Todos os componentes dos equipamentos devem ser do próprio fabricante ou estar em conformidade com a sua política de garantia, não sendo permitida a integração de itens de terceiros que possam acarretar perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada**
11.25	**A empresa fabricante do equipamento deverá prover assistência técnica onsite na sede da contratante ou no local de instalação do equipamento, devendo ser considerada como área de abrangência, quaisquer localidades dentro do Estado de domicílio da mesma;**
11.26	**A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos;**
11.27	**A empresa fabricante do equipamento deverá possuir um sistema atendimento de suporte técnico via Chat, através da Internet;**
11.28	**A empresa fabricante do equipamento deverá possuir um sistema de diagnóstico de hardware através do web site ou sistema próprio.**

A.12. ESPECIFICAÇÕES DO ITEM 12* (CATSER 27472)

*** Cota principal – item relacionado ao item 9 (cota reservada) para fins do disposto no §3º do art. 8º do Decreto nº 8.538/2015".**

ITEM 12 – LICENÇA DE MICROSOFT WINDOWS SERVER DATACENTER
12 MICROSOFT WINDOWS SERVER DATACENTER
12.1 Licenciamento Microsoft Windows Server Datacenter por pacotes com 2 cores;
12.2 Deve ser fornecida licença da versão mais atual do software, com possibilidade de downgrade para a versão 2019
12.3 O suporte técnico deverá ser balcão, de 12 meses.

A.13. ESPECIFICAÇÕES DO ITEM 13* (CATSER 27472)

***Cota principal – item relacionado ao item 10 (cota reservada) para fins do disposto no § 3º do art. 8º do Decreto nº 8.538/2015".**

ITEM 10 – LICENÇA CAL DE MICROSOFT WINDOWS SERVER
13 MICROSOFT WINDOWS SERVER CAL
13.1 Licenciamento CAL do Microsoft Windows Server por dispositivo;
13.2 Deve ser fornecida licença da versão mais atual do software, com possibilidade de downgrade para a versão 2019
13.3 O suporte técnico deverá ser balcão, de 12 meses.