TRIBUNAL REGIONAL ELEITORAL DA BAHIA
Seção de Contratos

ATA DE REGISTRO DE PREÇOS N.º 14/2022

PROCESSO (SEI) N.º 0015838-60.2021.6.05.8000

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, neste ato representado pelo seu Diretor-Geral, Raimundo de Campos Vieira, considerando o resultado do Pregão Eletrônico n.º 02/2022, cujo objeto se constitui no Registro de Preços para eventual aquisição de equipamentos e programas de datacenter, RESOLVE, com amparo nas Leis nº 8.666/93 e n.º 10.520/2002, nos Decretos n.ºs 10.024/2019 e 7.892/2013, e na Resolução Administrativa n.º 10/2007 do TRE da Bahia, registrar os preços da 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, **indicados no Anexo I desta Ata**, observadas as condições do Edital que integra este instrumento de registro, independentemente de transcrição.

Será incluído nesta Ata, no Anexo II, o registro das **licitantes** que aceitaram cotar os bens ou serviços com preços iguais aos da **licitante vencedora** na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei n.º 8.666/93.

O prazo de validade improrrogável da Ata de Registro de Preços é de 12 (doze) meses, contado da data da sua assinatura, excluído o dia do começo e incluído o do vencimento.

A assinatura da presente Ata implicará na plena aceitação, pelo fornecedor, das condições estabelecidas no Edital da licitação e seus anexos.

A licitante vencedora somente será liberada, sem penalidade, do compromisso previsto nesta Ata, nas hipóteses previstas no art. 18, § 1º, art. 19, inciso I e art. 21, incisos I e II, do Decreto n.º 7.892/2013.

REAJUSTE: 1. 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. **2.** 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. **3.** Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial para reajustamento dos preços. **4.** 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.

Passam a fazer parte desta Ata, para todos os efeitos, a documentação e propostas apresentadas pela licitante.

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 ajuste.

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.

TRIBUNAL REGIONAL ELEITORAL DA BAHIA:05967350000145
Assinado de forma digital por TRIBUNAL REGIONAL ELEITORAL DA BAHIA:05967350000145
Dados: 2022.04.18 08:43:45 -03'00'

HERBERT JOSE AZEVEDO:10260365858
Assinado de forma digital por HERBERT JOSE AZEVEDO:10260365858
Dados: 2022.04.12 09:34:41 -03'00'

Raimundo de Campos Vieira
Diretor-Geral do TRE-BA

Herbert José Azevedo
CPF Nº 102.603.658-58
PTLS SERVIÇOS DE TECNOLOGIA E ASSESSORIA TÉCNICA LTDA

FABIO CUNHA:27338922829
Assinado de forma digital por FABIO CUNHA:27338922829
Dados: 2022.04.12 10:02:00 -03'00'

Fábio Cunha
CPF Nº 273.389.228-29
PTLS SERVIÇOS DE TECNOLOGIA E ASSESSORIA TÉCNICA LTDA

ANEXO I – PREÇOS

Item	Descrição	Quantidade	Valor Unitário (R$)	Valor Total (R$)
5	Appliance Virtual de Balanceamento de Carga com Firewall de Aplicações. As especificações detalhadas constam no Anexo A do Termo de Referência.	02 unidades	498.000,00	996.000,00

ANEXO II – CADASTRO DE RESERVA

Não houve Cadastro de Reserva.

ANEXO III – 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	01 unidade

ITEM	DESCRIÇÃO	QUANTIDADE
	Professional. As especificações detalhadas constam no Anexo A deste Termo de Referência.	
9	Licença de Windows Server Datacenter 2019. As especificações detalhadas constam no Anexo A deste Termo de Referência.	7 unidades
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.

ESPECIFICAÇÕES DO ITEM 5 (CATSER 27472)

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.	**SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES**
1.1	**GERAL**
1.1.1	**Suportar e garantir a instalação em ambiente de alta disponibilidade;**
1.1.2	**A solução ofertada deva trabalhar simultaneamente em diversos modos de operação: Passivo, Ativo, Proxy reverso e Proxy transparente**
1.1.3	**Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo;**
1.1.4	**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;**
1.1.5	**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;**
1.1.6	**Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;**
1.1.7	**A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes**
1.1.8	**O equipamento deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda antes de qualquer equipamento de segurança ;**
1.1.9	**Fornecer recurso de agregação de portas baseado no protocolo LACP**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.1.10	**Deve possuir suporte a LACP em modo passivo e ativo**
1.1.11	**Fornecer recurso para suportar até 32 portas em um mesmo conjunto agregado;**
1.1.12	**Deve possuir suporte a Spanning-Tree(802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s)**
1.1.13	**Fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;**
1.1.14	**Possuir suporte a IPv6;**
1.1.15	**A solução deve suportar múltiplas tabelas de rotas independentes;**
1.1.16	**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;**
1.1.17	**Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SLB, GSLB, Aceleração Web, etc.**
1.1.18	**A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;**
1.1.19	**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.**
1.1.20	**Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).**
1.1.21	**Gerenciamento da Solução**
1.1.22	**Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;**
1.1.23	**Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);**
1.1.24	**Permitir acesso in-band via SSH;**
1.1.25	**Manter internamente múltiplos arquivos de configurações do sistema;**
1.1.26	**Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;**
1.1.27	**Possuir auto-complementação de comandos na CLI;**
1.1.28	**Possuir ajuda contextual;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.1.29	Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;
1.1.30	Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;
1.1.31	Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;
1.1.32	Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;
1.1.33	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.
1.1.34	Possuir Interface Gráfica via Web;
1.1.35	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;
1.1.36	A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;
1.1.37	Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
1.1.38	Suportar a rollback de configuração e imagem;
1.1.39	Permitir integração com a plataforma HP OpenView;
1.1.40	Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;
1.1.41	Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;
1.1.42	Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;
1.1.43	A interface Gráfica deverá permitir a reinicialização do equipamento;
1.1.44	Reinicialização do equipamento por comando na CLI;
1.1.45	Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;
1.1.46	Possuir traps SNMP;
1.1.47	Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics,

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	history, alarms e events
1.1.48	**Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;**
1.1.49	**Implementar Debugging: CLI via console e SSH;**
1.1.50	**Deve possuir suporte a Link Layer Discovery Protocol (LLDP);**
1.1.51	**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;**
1.1.52	**A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;**
1.1.53	**A Solução deve ter suporte a sFlow;**
1.2	**BALANCEAMENTO**
1.2.1	**Suportar todas as aplicações comuns de um Switch Layer 7, como:**
1.2.1.1	**Server Load-Balancing;**
1.2.1.2	**Firewall Load-Balancing;**
1.2.1.3	**Proxy Load-Balancing;**
1.2.2	**Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;**
1.2.3	**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;**
1.2.4	**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;**
1.2.5	**Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;**
1.2.6	**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.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.2.7	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.
1.2.8	Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.
1.2.9	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;
1.2.10	Suportar os seguintes métodos de balanceamento:
1.2.10.1	Round Robin;
1.2.10.2	Least Connections;
1.2.10.3	Weighted Percentage (por peso);
1.2.10.4	Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
1.2.10.5	Weighted Percentage dinâmico (baseado no número de conexões)
1.2.10.6	Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;
1.2.11	A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;
1.2.12	Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
1.2.12.1	Por cookie: inserção de um novo cookie na sessão;
1.2.12.2	Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
1.2.12.3	Por endereço IP destino;
1.2.12.4	Por endereço IP origem;
1.2.12.5	Por sessão SSL;
1.2.12.6	Através da análise da URL acessada.;
1.2.12.7	Através da análise de qualquer parâmetro no header HTTP;
1.2.12.8	Através da análise do MS Terminal Services Session (MSRDP)

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.2.12.9 Através da análise do SIP Call ID ou Source IP;
1.2.12.10 Através da análise de qualquer informação da porção de dados (camada 7);
1.2.13 A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;
1.2.14 O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
1.2.14.1 Layer 3 – ICMP;
1.2.14.2 Conexões TCP e UDP pela respectiva porta no servidor;
1.2.15 - 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;
1.2.16 Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);
1.2.17 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;
1.2.18 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;
1.2.19 Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;
1.2.20 Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
1.2.21 Realizar Network Address Translation (NAT);
1.2.22 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.
1.2.23 Realizar Proteção contra Denial of Service (DoS);
1.2.24 Realizar Proteção contra Syn flood;
1.2.25 Realizar Limpeza de cabeçalho HTTP;
1.2.26 A solução deve permitir o controle da resposta ICMP por servidor virtual;
1.2.27 Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;
1.2.28 Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.2.29	Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;
1.2.30	Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
1.2.31	Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);
1.2.32	Possuir capacidade para definir compressão especificamente para certos tipos de objetos;
1.2.33	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;
1.2.34	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;
1.2.35	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.
1.2.36	Deve possuir a funcionalidade de espelhamento de conexões SSL.
1.2.37	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.
1.2.38	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;
1.2.39	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:
1.2.40	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;
1.2.41	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

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	do túnel SSL/TLS;
1.2.42	**Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;**
1.2.43	**Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:**
1.2.43.1	**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;**
1.2.43.2	**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;**
1.2.44	**A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;**
1.2.45	**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;**
1.2.46	**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:**
1.2.46.1	**SSL session cache Timeout**
1.2.46.2	**Session Ticket;**
1.2.46.3	**OCSP (Online Certificate Status Protocol) Stapling;**
1.2.46.4	**Dynamic Record Sizing;**
1.2.46.5	**ALPN (Application Layer Protocol Negotiation);**
1.2.46.6	**Perfect Forward Secrecy;**
1.2.47	**Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;**
1.2.48	**Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;**
1.2.49	**Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.2.50 Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;
1.2.51 A solução deve suportar Internet Content Adaptation Protocol (ICAP);
1.2.52 Deve ser capaz de realizar DHCP relay;
1.2.53 Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:
1.2.53.1 Tempo de resposta da aplicação;
1.2.53.2 Latência;
1.2.53.3 Conexões para conjunto de servidores, servidores individuais;
1.2.53.4 Por URL;
1.2.54 A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:
1.2.55 Servidores virtuais
1.2.56 Servidores balanceados
1.2.57 URLs
1.2.58 Países de origem, baseados em geolocalização (GEOIP)
1.2.59 Dispositivos de origem do cliente (user agent)
1.2.60 Deve possuir framework unificado para configuração da aplicação
1.2.61 Deve possuir criptografia IPSEC para comunicação entre os balanceadores;
1.2.62 Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;
1.2.63 A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;
1.2.64 A Solução deve ter suporte a sFlow;
1.2.65 A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;
1.2.66 A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
1.2.67 A solução deve suportar Equal Cost Multipath (ECMP);
1.2.68 A solução deve realizar Bidirectional Forward Detection (BFD);

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.2.69	A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);
1.2.70	Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);
1.2.71	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;
1.2.72	A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;
1.2.73	A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
1.2.74	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:
1.2.74.1	Deve ser possível configurar o tamanho máximo da fila;
1.2.74.2	Deve ser possível configurar o tempo máximo de permanência na fila;
1.2.75	A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;
1.2.76	A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário;
1.2.77	A solução deve realizar Controle de Banda baseado em domínio de roteamento;
1.2.78	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;
1.2.79	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.
1.2.80	A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
1.2.81	A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;
1.2.82	A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;
1.2.83	Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;
1.2.84	Possuir suporte ao protocolo SPDY e HTTP 2.0;
1.2.85	O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.2.86 O equipamento deverá permitir a sincronização das configurações:
1.2.86.1 De forma automática;
1.2.86.2 Manualmente, forçando a sincronização apenas no momento desejado;
1.2.87 Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:
1.2.87.1 Compartilhar a rede de heartbeat com a rede de dados;
1.2.87.2 Utilizar uma rede exclusiva para o heartbeat.
1.2.88 Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
1.2.89 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.
1.2.90 Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:
1.2.91 GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version
1.2.92 Deve ser possível tomar as seguintes ações através dessas políticas:
1.2.93 Bloqueio de tráfego
1.2.94 Reescrita e manipulação de URL
1.2.95 Registro de tráfego (log)
1.2.96 Adição de informação no cabeçalho HTTP
1.2.97 Redirecionamento do tráfego para um membro específico
1.2.98 Selecionar uma política específica para Aplicação Web
1.2.99 A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:
1.2.99.1 Endereço IP de origem;
1.2.99.2 Porta TCP ou UDP de origem;
1.2.99.3 Endereço IP de destino;
1.2.99.4 Porta TCP ou UDP de destino;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.2.99.5 Protocolo de camada 4 (TCP ou UDP);
1.2.99.6 Data e hora da mensagem;
1.2.99.7 URL acessada;
1.2.100 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 de forma nativa ou no mínimo integrado a uma base Active Directory.
1.2.101 A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.
1.2.102 A solução deve ser capaz de analisar a performance de aplicações web.
1.2.103 A solução deve possuir relatórios das aplicações.
1.2.104 Deve prover métricas de aplicações como: Transações por Segundo;Tempo de latência do cliente e servidor;Throughput de requisição e resposta;Sessões
1.2.105 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.
1.2.106 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.
1.2.107 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.
1.2.108 A geração de informações históricas deverá permitir:
1.2.109 O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;
1.2.110 Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.
1.3 DNS
1.3.1 A solução deve operar em, no mínimo, a seguintes formas:
1.3.1.1 DNS autoritativo;
1.3.1.2 DNS secundário;
1.3.1.3 DNS resolver;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.3.1.4 DNS cache;
1.3.1.5 Balanceamento de DNS servers;
1.3.1.6 DNSSec;
1.3.2 A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas.
1.3.3 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;
1.3.4 A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;
1.3.5 A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;
1.3.6 A solução deve possuir certificação ICSA;
1.3.7 A solução deve possuir proteções contra ataques DNS, no mínimo:
1.3.8 - Inspeção de protocolo;
1.3.9 - Validação de protocolo;
1.3.10 - UDP flood;
1.3.11 - Pacotes mal formados;
1.3.12 - Ataque Teardrop;
1.3.13 - Ataque ICMP;
1.3.14 Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra ataques;
1.3.15 A solução deve ser capaz de realizar balanceamento dos servidores DNS;
1.3.16 A solução deve ser capaz de realizar filtragem de pacotes;
1.3.17 A solução deve prover segurança do protocolo DNS, protegendo contra ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS .
1.3.18 A solução deve prover segurança do protocolo DNS, protegendo contra ataques de Cache Poisoning.
1.3.19 A solução deve realizar stateful inspection;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.3.20	A solução deve possuir base de Geolocalização IP;
1.3.21	A solução deve implementar DNS64;
1.3.22	A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT
1.3.23	Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;
1.3.24	Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;
1.3.25	Deve prover as respostas a queries DNS da própria RAM CACHE
1.3.26	A solução deve ser capaz de realizar IP Anycast;
1.3.27	A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso
1.3.28	A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;
1.3.29	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;
1.3.30	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;
1.3.31	Deve ser possível ajustar quantos endereços são enviados em uma única resposta;
1.3.32	Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;
1.3.33	Suportar pelo menos os seguintes algoritmos de balanceamento:
1.3.33.1	Round Robin;
1.3.33.2	Global Availability;
1.3.33.3	Ratio;
1.3.33.4	LDNS Persist;
1.3.33.5	Geografia;
1.3.33.6	Disponibilidade da Aplicação;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.3.33.7 Capacidade do Virtual Server;
1.3.33.8 Least Connections;
1.3.33.9 Pacotes por segundo;
1.3.33.10 Round trip time;
1.3.33.11 Hops;
1.3.33.12 Packet Completion Rate
1.3.33.13 QoS definido pelo usuário;
1.3.33.14 Kilobytes per Second;
1.3.34 Implementar persistência da conexão do usuário entre aplicações ou data centers;
1.3.35 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;
1.3.36 A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;
1.3.37 A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual;
1.3.38 A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);
1.3.39 Possuir suporte a IPv6 no balanceamento global entre datacenters.
1.3.40 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.
1.3.41 Deverá possuir a funcionalidade de resposta rápida a queries DNS. permitindo respostas mais rápidas para zonas que seja autoritativo.
1.3.42 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.
1.3.43 A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (GSLB) ou encaminhar requisições de clientes (screening).

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.3.44	**Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões.**
1.3.45	**A solução deve funcionar pelo menos das seguintes formas:**
1.3.46	**Usar o ECS para tomar decisões de GSLB baseado em topologia (Subnets)**
1.3.47	**Injetar o ECS (proxy requests) para outros servidores DNS**
1.3.48	**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.**
1.3.49	**Serviço de DNS com Firewall DNS**
1.3.50	**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.**
1.3.51	**Infraestrutura de hardware e software destinada à função de resolução de nomes DNS de uso exclusivo da CONTRATANTE.**
1.3.52	**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.**
1.3.53	**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.**
1.3.54	**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.**
1.3.55	**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).**
1.3.56	**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.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.3.57	O serviço deve ter, pelo menos, as seguintes características de segurança:
1.3.58	Deve permitir o uso de lista negra para bloquear domínios DNS.
1.3.59	Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas.
1.3.60	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 possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet).
1.3.61	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.
1.3.62	Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio.
1.3.63	A solução deverá suportar mecanismo de “assinaturas”, ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento.
1.3.64	O serviço deverá permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:
1.3.65	Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP.
1.3.66	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.
1.3.67	Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado.
1.3.68	De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP.
1.3.69	Criar “Listas brancas” que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem.
1.3.70	O serviço deverá proteger contra os seguintes ataques de DNS:
1.3.71	Reflexão.
1.3.72	Anomalias de Protocolo.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.3.73 Negação de Serviço.
1.3.74 Negação de Serviços Distribuídos.
1.3.75 Amplificação.
1.3.76 Tunelamento.
1.3.77 Reconhecimento.
1.3.78 Explorações (Exploit).
1.3.79 Envenenamento do cache.
1.3.80 Excessos (Floods).
1.3.81 O serviço deve permitir que os administradores efetuem busca de endereços de rede, subrede e endereços IP através de filtros.
1.3.82 A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração.
1.3.83 O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup.
1.3.84 O serviço deverá fornecer pelo menos os seguintes relatórios:
1.3.85 Tendência de latência de resposta de DNS.
1.3.86 Nomes de domínios de DNS mais requisitados.
1.3.87 Tendência de uso do cache de DNS.
1.3.88 Top clientes de DNS.
1.3.89 Taxa de consultas de DNS por tipo de registro.
1.3.90 Tendências de respostas de DNS.
1.3.91 Taxa de consultas de DNS diária por servidor.
1.3.92 Pico de consultas diárias de DNS por servidor.
1.3.93 Top DNS NXDOMAIN/No error.
1.3.94 Top SERVFAIL enviados e recebidos.
1.3.95 Top clientes por domínio de DNS.
1.3.96 Nomes de domínios com conteúdo malicioso.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.3.97 Principais domínios maliciosos.
1.3.98 Principais acessos ao DNS Firewall.
1.3.99 Quantidade de eventos registrados por horário.
1.3.100 Quantidade de eventos por severidade.
1.3.101 Quantidade de eventos por regra.
1.3.102 Quantidade de eventos por tendência.
1.3.103 Quantidade de eventos por categoria.
1.3.104 Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições.
1.3.105 Deve implementar DNSSEC com suporte a NSEC3 (RFC 5155).
1.4 FIREWALL DE DATA CENTER
1.4.1 A solução deve atuar como stateful firewall;
1.4.2 solução deve atuar como full-proxy;
1.4.3 A solução deve permitir a criação de logs customizados por aplicação;
1.4.4 A solução deve terminar as conexões SSL com a finalidade de inspecioná-las;
1.4.5 A solução deve proteger de ataques DDoS nas camadas de rede e de sessão;
1.4.6 A solução deve possuir linguaguem de programação que garanta a flexibilidade;
1.4.7 A solução deve proteger de ataques DDoS que utilizem SSL
1.4.8 A solução deve permitir a criação de regras com, no mínimo, os seguintes parâmetros:
1.4.9 - Endereço IP destino
1.4.10 - Endereço IP de origem
1.4.11 - Porta de destino
1.4.12 - Porta de origem
1.4.13 - VLAN
1.4.14 - Protocolo
1.4.15 - Ação
1.4.16 - Horário

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.4.17	**- Log**
1.4.18	**A solução deve permitir definir agendamento para ativação da regra;**
1.4.19	**A solução deve permitir definir, no mínimo, as seguintes ações no tráfego:**
1.4.20	**- Permitir: os pacotes são aceitos e passam pelo firewall;**
1.4.21	**- Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;**
1.4.22	**- Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;**
1.4.23	**Deve ser possível criar regras que sejam aplicadas em diferentes pontos, no mínimo:**
1.4.24	**- Global;**
1.4.25	**- Domínio de Roteamento;**
1.4.26	**- Virtual Server;**
1.4.27	**Deve possuir criptografia IPSEC para comunicação entre os sites.**
1.4.28	**Permitir a configuração de múltiplas contas de usuário local;**
1.4.29	**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;**
1.4.30	**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.**
1.4.31	**Permitir a restauração das configurações de proteções originais;**
1.4.32	**Permitir a configuração em alta disponibilidade;**
1.4.33	**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**
1.4.34	**Deve permitir criar lista de exceção de regras (whitelist/blacklist) por endereço IP específico ou faixa de sub-rede**
1.4.35	**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.**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.4.36	Todas as licenças de uso permanentes necessárias para possibilitar o seu funcionamento de acordo com as especificações definidas
1.4.37	Todos os softwares devem ser entregues com cessão de direito de uso permanente, para usuários ilimitados.
1.4.38	Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito;
1.4.39	Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;
1.4.40	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;
1.4.41	Bloqueio de ataques em serviços HTTP;
1.4.42	Descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período de tempo configurável;
1.4.43	Bloqueio de requisições DNS na porta 53 malformadas
1.4.44	Limitar o número de consultas DNS por segundo através da configuração de uma taxa (thresholds)
1.4.45	Detectar e descartar pacotes HTTP que não atendam aos padrões RFC e, em seguida, barrar os hosts de origem;
1.4.46	Executar a atualizações necessárias para prevenção de novos ataques;
1.4.47	Mitigar, no mínimo, os seguintes tipos de ataques:
1.4.48	ICMP/UDP/TCP FloodS;
1.4.49	TCP Flag Abuses;
1.4.50	GET/POST FloodS;
1.4.51	SYN Floods;

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES
1.4.52 UDP Bandwidth Attacks;
1.4.53 Smurfing;
1.4.54 NTP Reflection Attacks;
1.4.55 TCP/UDP Bandwidth Attacks;
1.4.56 Fragging Attack;
1.4.57 Slowloris;
1.4.58 Connection Attacks;
1.4.59 Botnet;
1.4.60 Fragmentation attacks;
1.4.61 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.
1.4.62 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.
1.4.63 A solução deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DoS.
1.4.64 Deve possuir suporte ao envio de SNMP traps para cada ataque DoS detectado.
1.5 WAF
1.5.1 A solução deve operar nos modos ativo-ativo e ativo-standby;
1.5.2 O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7);
1.5.3 Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
1.5.4 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.
1.5.5 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.

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.5.6	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.
1.5.7	O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);
1.5.8	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.
1.5.9	Possuir política de segurança de aplicações web pré-configurada na solução.
1.5.10	Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
1.5.11	Permitir a criação de políticas diferenciadas por aplicação.
1.5.12	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;
1.5.13	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;
1.5.14	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.
1.5.15	A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;
1.5.16	Essa inspeção pode ser feito via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus;
1.6	GARANTIA DO PRODUTO:
1.7	Os produtos devem possuir licenciamento perpétuo, garantia e suporte do fabricante por 60 (sessenta) meses;
1.8	A garantia do produto deve iniciar-se conforme descrito nos prazos deste Termo de Referência.
1.9	A garantia deve compreender:
1.10	A troca do equipamento ou algum de seus componentes em caso de falha, como defeito de fabricação, panes elétricas de peças, entre outros;
1.11	Disponibilização de correção de falhas, atualização dos produtos, incluindo vacinas,

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
	assinaturas, bases de dados sem ônus adicional para a CONTRATANTE;
1.12	**Prazos para troca de equipamentos ou componentes:**
1.13	**4 horas para o caso de indisponibilidade total da solução;**
1.14	**72 horas para os demais casos;**
1.15	**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.**
1.16	**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;**
1.17	**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;**
1.18	**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;**
1.19	**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:**
1.20	**Patches, fixes, correções, updates e servicepacks;**
1.21	**Novas releases, builds e funcionalidades;**
1.22	**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;**
1.23	**O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência da garantia;**
1.24	**A correção de falhas do fabricante deve incluir:**
1.25	**Atualização do sistema (software upgrades);**
1.26	**A correção de falhas do fabricante deve incluir:**
1.27	**Atualização do sistema (software upgrades);**
1.28	**Assistência remota online e por telefone;**

ITEM 5 – SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES	
1.29	**Assistência proativa para manutenção planejada;**
1.30	**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;**
1.31	**Recebimento, por e-mail, alertas de segurança sobre questões relacionadas à ferramenta;**
1.32	**Qualquer ação para atualização deve ser realizada com anuência da CONTRATANTE;**
1.33	**SERVIÇOS DE IMPLANTAÇÃO:**
1.34	**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;**
1.35	**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);**
1.36	**A CONTRATADA deverá fornecer o(s) certificado(s) digital(is) SSL necessários para o funcionamento do software.**