ILUSTRÍSSIMO SENHOR(A) PREGOEIRO(A)/ PRESIDÊNCIA DO TRE-PI

PREGÃO ELETRÔNICO Nº 011/2023

Processo Administrativo Nº 0020437-45.2022.6.18.8000

Objeto: Escolha da melhor proposta de preços para aquisição futura de Solução de Web Application Firewall (WAF) e balanceamento de carga, incluindo serviços de implantação, transferência tecnológica (hands-on), treinamento especializado, operação assistida e garantia da solução por 60 (sessenta) meses.

A Imagetech Tecnologia em Informática Ltda, pessoa jurídica de direito privado interno, empresa sediada à rua 15 de Novembro, 2.668, Loja, anexo ao Edifício Terrace Tower, Bairro Jardim dos Estados, CEP 79020-300, na cidade de Campo Grande, Estado de Mato Grosso do Sul, telefone e fax (67) 3357-0700, e-mail licitacao@grupoimagetech.com.br, inscrita no CNPJ sob n. 05.583.680/0001-37, inscrição estadual nº 28.326.487-0, já qualificada, ora denominada Recorrente, vem mui respeitosamente à presença de V. Sa. Interpor o presente recurso administrativo.

Precipuamente esclarece a Recorrente que a interposição do presente Recurso Administrativo é o exercício do direito e da garantia constitucional do contraditório e da ampla defesa, jamais havendo por parte desta empresa o interesse em tentativa de frustrar o procedimento licitatório, ao contrário, o objetivo sempre foi e será de que este ocorra dentro dos ditames legais, sob a égide dos sagrados e basilares princípios da legalidade e da igualdade.

RECURSO ADMINISTRATIVO

I – DA TESPESTIVIDADE

Inicialmente, cabe destacar que nos termos do inciso XVIII do art. 4º da Lei 10.520/2002, bem como o item 13.1 do edital que rege o pregão eletrônico supra citado, uma vez declarado o vencedor, qualquer licitante poderá manifestar imediata e motivadamente a intenção de recorrer, quando lhe será concedido o prazo de 3 (três) dias para apresentação das razões do recurso. Verifica-se do procedimento administrativo em tela que a Recorrente teve a sua intenção de recurso devidamente aceita em 23/05/2023 (terça-feira), apontando-se ainda que o prazo para a Recorrente apresentar suas razões recursais iniciou-se no mesmo dia, pelo que findar-se-á em 26/05/2023 (sexta-feira).

II – DAS RAZÕES RECURSAIS:

A Recorrente, participante do presente processo licitatório (grupo único), apresentou menor oferta com substancial diferença para o segundo colocado, porém foi inabilitada nos seguintes termos:

Eventos do Item

Evento	Data	Observações
Recusa de proposta	19/05/2023 08:34:25	Recusa da proposta. Fornecedor: IMAGETECH TECNOLOGIA EM INFORMATICA LTDA, CNPJ/CPF: 05.583.680/0001-37, pelo melhor lance de R$ 562.000,0000. Motivo: Consoante parecer da Unidade técnica, documentação apresentada não comprova que o produto ofertado atende às especificações exigidas no instrumento convocatório.
Aceite de proposta	23/05/2023 09:40:32	Aceite individual da proposta. Fornecedor: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA., CNPJ/CPF: 02.092.332/0001-79, pelo melhor lance de R$ 563.000,0000.
Habilitação de fornecedor	23/05/2023 09:57:07	Habilitação em grupo de propostas. Fornecedor: CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA. - CNPJ/CPF: 02.092.332/0001-79

Saliente-se que o objetivo da Administração Pública ao iniciar um processo licitatório é exatamente obter proposta mais vantajosa para contratação de bem ou serviço que lhe seja necessário, observados os termos da legislação aplicável.

Ainda, em contraparte, na fl. 10, item "9" (Edital Pregão Eletrônico nº 11/2023) não há citação de que a documentação técnica demonstrada na fl. 49, item "4.3 e 4.6" fosse de extrema necessidade, já que a mesma é citada apenas no Termo de Referência e não no documento convocatório. Portanto, essa deliberação causará danos a Administração Pública, no que se refere ao valor da contratação, visto que o propósito do instrumento convocatório é alcançar a proposta mais vantajosa. Diante disso, a empresa habilitada não possui esse requisito, já que apresenta uma asserção de cotação superior a inicial da recorrente, acarretando uma diferença de R$ 240.724,80 (duzentos e quarenta mil, setecentos e vinte e quatro reais e oitenta centavos).

Quadro comparativo de propostas	
CNPJ/CPF: 05.583.680/0001-37 - IMAGETECH TECNOLOGIA EM INFORMATICA LTDA	R$2.250.000,00
CNPJ/CPF: 02.092.332/0001-79 - CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA	R$2.490.724,80

Vale ressaltar que, a recorrente tem total qualificação técnica para o atendimento do objeto do certame, uma vez que a empresa já havia desempenhado e conquistado outros certames de objetos similares e atendeu aos requisitos pré-estabelecidos, conforme comprovado em Atestado de Capacidade Técnica enviado na habilitação.

A Recorrente entende que o envio da documentação **adicional**, conforme descrito no Termo de Referência, denominado documento ponto a ponto, em um prazo máximo de 48 horas, seria totalmente amparado pelo princípio da razoabilidade, considerando que a proposta obteve um desconto considerável sobre o valor ofertado pelo segundo colocado.

Podemos citar claramente o trecho do Anexo I do Edital – "Termo de Referência n. 11/2023", que demonstra que esse documento ponto a ponto é um documento "**adicional**", não exigida no subitem 4.3.2, alínea 'b' do Edital.

Texto extraído do Edital, Item 4:

> *"4. DO ENVIO DA PROPOSTA*
>
> *...*
>
> *4.3.1. Marca e modelo, preço unitário e total dos itens;*
>
> *4.3.2. Descrição detalhada do objeto, contendo as informações similares à especificação do Termo de Referência indicando, no que for aplicável:*
>
> *...*
>
> *b) Especificação dos bens ofertados, forma de acondicionamento do bem, quantidade, prazo de validade. Sugerimos encaminhar catálogo, folder ou link de sites onde a Unidade responsável possa confirmar as características;"*

Texto extraído do Termo de Referência, Item 4 e 4.3:

> *"4. APRESENTAÇÃO DA PROPOSTA E CRITÉRIO DE JULGAMENTO (Termo de Referência)*
>
> *...*
>
> *4.3. A proposta da licitante deverá vir acompanhada de documentação técnica que comprove o atendimento de todos os requisitos deste termo de referência. Para tal, deverá ser indicado na proposta comercial os part number(s) referente(s) a cada equipamento, softwares fornecidos, licenças de uso e garantia do produto.*
>
> ***Adicionalmente**, a licitante deverá indicar, ponto a ponto, qual seção da documentação técnica comprova o atendimento de cada requisito e conformidade do material proposto com a especificação exigida deste termo de referência, evitando a pura transcrição do disposto neste Termo de Referência para a proposta."*

Neste mesmo sentido, para comprovação do subitem 4.6 do Termo de Referência, poderia ser concedido o envio do documento em prazo mais razoável, considerando que o equipamento ofertado é completamente aderente aos requisitos ambientais e que não possuem substancias perigosas em sua fabricação, como podemos constatar no catálogo do produto enviado juntamente com a proposta, arquivo "*LoadMaster-HW (1).en.pt.pdf*", página 13:

	LM-X15/LM-X15-MT
FIPS	FIPS 140-2 Nível 1 NIST Cert 2473
Aprovação da Agência de Segurança: (IEC, EN, CSA, UL)	IEC 62368-1:2014 2ª Ed. EN 62368-1:2014+A11:2017 AS/ NZS 62368.1:2018 CAN/CSA C22.2 No. 62368-1-14 UL 62368-1 2ª Ed.
Certificações de compatibilidade eletromagnética (EMC): (CE, UKCA, FCC, VCCI)	EN 55032:2015 +AC:2016, Classe A EN 55032:2012 +AC:2013, Classe A EN 61000-3-2:2014, Classe A EN 61000-3-3:2013 EN 55035:2017 CISPR 32:2015+COR1:2016 AS/NZS CISPR 32:2015, Classe A 47 CFR FCC Parte 15 Subparte B, Classe A ICES-003:2016 Edição 6, atualizado em abril de 2019 Classe A ANSI C63.4:2014 VCCI-CISPR 32:2016, Classe A
Compatível com RoHS	Sim
Compatível com WEEE	Sim
Compatível com REACH	Sim

No catalogo do produto ofertado, e enviado juntamente com a proposta, é claramente especificado que o equipamento é compatível com a RoHS. O RoHS (Restrictions of the use of Certain Hazardous Substances) se trata de restrição ao uso de substâncias perigosas em artefatos (produtos ou equipamentos) eletroeletrônicos, comercializados nos estados-membros da UE, proibindo a entrada de novos produtos no mercado caso contenham chumbo, cádmio, cromo hexavalente, mercúrio, bifenilas polibromadas (PBB) e éteres difenílicos polibromados (PBDE). https://www.ipt.br/solucoes/30-analises_quimicas_para_adequacao_a_diretiva_rohs.htm

Bem como o equipamento é compatível com o REACH, que é um regulamento da União Europeia adotado para melhorar a proteção da saúde humana e do ambiente face aos riscos que podem resultar dos produtos químicos, contribuindo ao mesmo tempo para reforçar a competitividade da indústria química da União Europeia. https://echa.europa.eu/pt/regulations/reach/understanding-reach

Quanto ao terceiro e último item apontado para a desclassificação da recorrente, "3. por último, verificamos que os atestados de capacidade técnica apresentados pela empresa comprovam, em nosso entendimento, os conhecimentos necessários sobre produtos de fabricante diferente do fabricante do equipamento ofertado ao Tribunal pela LICITANTE e não sobre os equipamentos oferecidos à este Tribunal", o item 5.4.1 do edital é bem claro quando cita que o atestado de capacidade tem como fim comprovar a aptidão para desempenho de atividade pertinente e **compatível** com o objeto da licitação.

> *"5.4.1. A LICITANTE deverá apresentar atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que comprove o fornecimento e implantação de, pelo menos, 01 (um) appliance virtual e/ou físico da solução Web Application Firewall (WAF), a fim de comprovar a*

aptidão para desempenho de atividade pertinente e compatível com o objeto da licitação;"

A requerente entende que atendeu a todos os requisitos exigidos no Edital, ofertou o melhor preço para a solução a ser contratada e solicitou à Administração apenas razoabilidade quanto ao prazo de entrega dessa documentação considerada ADICIONAL, conforme podemos verificar nos pontos demonstrados.

Isso posto, com a desclassificação da melhor proposta (com larga margem), motivado pela não concessão de prazo razoável (48 horas), considerando que apenas o prazo para apresentação das motivações dessa peça recursal e das contrarrazões superam muito ao prazo requerido por esta licitante para entrega da documentação adicional (06 dias ao todo).

Entretanto, os itens 10.1 e 10.2 do edital, contemplam:

> "10.1. Caso convocada pelo Pregoeiro, a proposta vencedora ajustada ao lance dado, conforme modelo constante no Anexo II deste Edital, será imediatamente encaminhada pelo sistema ComprasNet, no prazo razoável não inferior a 2 (duas) horas, a ser definido pelo Pregoeiro."
> "10.2. Os documentos complementares necessários à confirmação daqueles exigidos neste edital para habilitação deverão ser anexados ao ComprasNet no prazo não inferior a 2 (duas) horas contadas da convocação do anexo, a ser definido pelo Pregoeiro."

III – **DA FUNDAMENTAÇÃO**

Pelos princípios da economicidade, razoabilidade e formalismo moderado, e ainda, como o próprio item 24.4.1 do termo de referência, sustenta:

> "Consoante Acórdão TCU nº 1211/2021 – Plenário, o Pregoeiro, durante as fases de julgamento das propostas e/ou habilitação, deve sanear eventuais erros ou falhas que **não alterem a substância das propostas, dos documentos e sua validade jurídica**, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, nos termos dos arts. 8º, inciso XII, alínea "h"; 17, inciso VI; e 47 do Decreto 10.024/2019; sendo que a vedação à inclusão de novo documento, prevista no art. 43, § 3º, da Lei 8.666/1993 e no art. 64 da Nova Lei de Licitações (Lei 14.133/2021), não alcança documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta, que não foi juntado com os demais comprovantes de habilitação

> e/ou da proposta, por equívoco ou falha, o qual deverá ser solicitado e avaliado pelo Pregoeiro.” (Grifo nosso)

Inclusive, Marçal Justem Filho ensina sobre os princípios da proporcionalidade e da razoabilidade, os quais acarretam a impossibilidade de impor consequências de severidade incompatível com a irrelevância dos defeitos.

É de grande valia ressaltar que todos os julgados da Administração Pública estão embasados nos princípios insculpidos na legislação de regência.

É indiscutível que o Administrador responsável pela sessão pública deve sempre avaliar o conjunto de concorrentes, com a finalidade de evitar, a todo custo, inabilitações e/ou desclassificações precipitadas, cujos motivos ensejadores possam ser facilmente sanados. É de se esperar que aquele proceda com especial cautela na avaliação da documentação disponibilizada, já que lida com recursos públicos, sendo-lhe vedado levar a cabo exclusões sumárias e desarrazoadas.

Para tanto, prevê a Lei n° 8.666/93 ao falar de diligências:

> "Art. 43. A licitação será processada e julgada com observância dos seguintes procedimentos:
> (...)
> § 3°. É facultada à Comissão ou autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originalmente da proposta."

Cumpre destacar que o dispositivo legal citado em nada fere a vinculação ao instrumento convocatório e a necessidade de seu atendimento, tempestivamente, por todas as licitantes, desde que, é claro, novos documentos não sejam apresentados.

In casu, pode a D. Comissão de Licitação adotar o Princípio da Eficiência, visando buscar a seleção da proposta mais vantajosa para a Administração Pública, desde que observados os requisitos mínimos previamente estabelecidos, alcançando um padrão de qualidade, onde a vantagem correspondente será a de menor custo e maior benefício para a Administração.

No Acórdão n. 1211/2021, o Plenário do TCU estabeleceu a possibilidade de o licitante submeter novos documentos para suprir erro, falha ou insuficiência, a fim de viabilizar a seleção da proposta mais vantajosa, promovendo a competitividade e o formalismo moderado.

A vedação à inclusão de documento que deveria constar originariamente da proposta, nos termos do artigo 43, §3º, da Lei nº 8.666/1993, seria restrita ao documento que o licitante "não dispunha materialmente no momento da licitação".

Ou seja, a vedação não abarcaria condição atendida pelo licitante quando da apresentação da proposta e que não foi apresentada em conjunto com os demais comprovantes de habilitação ou da proposta, por equívoco ou falha —hipótese na qual o pregoeiro deverá promover o saneamento do erro.

O ministro Walton Alencar Rodrigues, destacou que:

> "(...) admitir a juntada de documentos que apenas venham a atestar condição pré-existente à abertura da sessão pública do certame não fere os princípios da isonomia e igualdade entre as licitantes e o oposto, ou seja, a desclassificação do licitante, sem que lhe seja conferida oportunidade para sanear os seus documentos de habilitação, resulta em objetivo dissociado do interesse público, com a prevalência do processo (meio) sobre o resultado almejado (fim)".

Nos termos do artigo 64 da Lei nº 14.133/2021:

> "Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:
>
> I - Complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame;
>
> II - Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.
>
> § 1º Na análise dos documentos de habilitação, a comissão de licitação poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante despacho fundamentado registrado e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.
>
> § 2º Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.".

Ressalte-se que para atender o Princípio da Eficiência, a Administração não pode, de maneira alguma, se entremear de excessos de formalismo, inclusive este entendimento já é bastante debatido em tribunais, sendo frequentes as decisões que prestigiam a adoção do princípio do formalismo moderado e a possibilidade de saneamento de falhas ao longo do procedimento licitatório.

Resumidamente, o formalismo moderado se relaciona à ponderação entre o princípio da eficiência e o da segurança jurídica, ostentando importante função no cumprimento dos objetivos descritos no art. 3º da lei de licitações: busca da proposta mais vantajosa para a Administração, garantia da isonomia e promoção do desenvolvimento nacional sustentável.

Nesse sentido, orienta o TCU no acórdão 357/2015-Plenário:

> "No curso de procedimentos licitatórios, a Administração Pública deve pautar-se pelo princípio do formalismo moderado, que prescreve a adoção de formas simples e suficientes para propiciar adequado grau de certeza, segurança e respeito aos direitos dos administrados, promovendo, assim, a prevalência do conteúdo sobre o formalismo extremo, respeitadas, ainda, as praxes essenciais à proteção das prerrogativas dos administrados."

Nota-se que sua utilização não significa desmerecimento ao princípio da vinculação ao instrumento convocatório ou negativa de vigência do caput do art. 41 da lei 8.666/93 que dispõe sobre a impossibilidade de a Administração descumprir as normas e condições do edital. Trata-se de solução a ser tomada pelo intérprete a partir de um conflito de princípios.

> "Diante do caso concreto, e a fim de melhor viabilizar a concretização do interesse público, pode o princípio da legalidade estrita ser afastado frente a outros princípios."
> (Acórdão 119/2016-Plenário)

Ao contrário do que ocorre com as regras/normas, os princípios não são incompatíveis entre si.

Diante de um conflito de princípios (p. ex., vinculação ao instrumento convocatório x obtenção da proposta mais vantajosa), a adoção de um não provoca a aniquilação do outro. Como exemplo, esse raciocínio pode ser percebido nas seguintes decisões do Tribunal de Contas da União:

> "Rigor formal no exame das propostas dos licitantes não pode ser exagerado ou absoluto, sob pena de desclassificação de propostas mais vantajosas, devendo as simples omissões ou irregularidades na documentação ou na proposta, desde que irrelevantes e não causem prejuízos à Administração ou aos concorrentes, serem sanadas mediante diligências."
> (Acórdão 2302/2012-Plenário)
> "O disposto no caput do art. 41 da Lei 8.666/1993, que proíbe a Administração de descumprir as normas e o edital, deve ser aplicado mediante a

> consideração dos princípios basilares que norteiam o procedimento licitatório, dentre eles o da seleção da proposta mais vantajosa."
> (Acórdão 8482/2013-1ª Câmara)

Nessas hipóteses, a análise deve considerar a importância de cada princípio no caso concreto, e realizar a ponderação entre eles a fim de determinar qual prevalecerá, sem perder de vista os aspectos normativos. Por esse motivo, as soluções não respeitam fórmulas prontas, podendo variar de um caso para outro.

A respeito do caso em comento, a D. Comissão tem a prerrogativa e pode realizar diligências para verificar a possibilidade de estar diante de um erro sanável, sendo este o caso desta recorrente, que é uma Licitante idônea, que apresentou uma proposta boa e de menor valor global, contendo as declarações, especificação de materiais, os preços de informações vitais para sua análise. É importante destacar que o fato de não termos anexado a Relação ponto a ponto e RoHS em nada afeta, ou altera, a essência da proposta.

O que também vale destacar é que em nenhum momento será ferido, violado, deixado de lado qualquer dos princípios basilares acerca do procedimento licitatório. Assim, inequívoco que diante de um aparente conflito de princípios, e diante de uma falha formal que não altera a substância e não onera o valor final, pode-se aplicar o princípio da ponderação, no caso em questão, por se tratar de um mero erro formal, e a Comissão pode solicitar seja sanado a qualquer tempo.

Nesse sentido, vale mencionar o ACORDÃO 2239/2018 – TCU

> "É irregular a desclassificação de proposta vantajosa à Administração por erro de baixa materialidade que possa ser sanado mediante diligência, por afrontar o interesse público".

E, por fim, importante destacar o princípio da eficiência na administração pública, eis que este aponta que o gestor público deve gerir a coisa pública com efetividade, economicidade, transparência e moralidade, visando cumprir as metas estabelecidas, e tudo isso se amolda ao caso em tela.

Nesse sentido, em relação à seleção da proposta mais vantajosa, este objetivo se traduz na necessidade que tem a Administração Pública de selecionar, dentre os critérios estabelecidos em edital, aquele que melhor atende as suas necessidades.

Portanto, não há o que se falar em desclassificação da proposta da recorrida por conta de mero erro sanável e excesso de formalismo.

No presente feito, cabe a realização de diligência por parte da D. Comissão, a fim de sanar, assim, eventual erro formal.

Diante da decisão do pregoeiro em nos debilitar, justificando ser em razão da não apresentação documental. O poder executivo optou por habilitar a empresa CLM SOFTWARE COMERCIO IMPORTACAO E EXPORTACAO LTDA CNPJ: 02.092.332/0001-79, onde o pregoeiro teve exigências excessivas.

IV – DOS PEDIDOS

ISTO POSTO, diante da plena comprovação de atendimento ao edital, REQUER, que os documentos que estão em anexo ao RECURSO (enviados para o e-mail cpl@tre-pi.jus.br, uma vez que o portal não detém campo para inclusão de anexos) sejam aceitos como documentação para complementar as informações dos já apresentados (de acordo com o **Acórdão n. 1211/2021**, já citado no início do Item III).

Conforme os fatos e argumentos apresentados neste **RECURSO,** solicitamos como lídima justiça que:

I – A peça recursal da recorrente seja conhecida para, **no mérito, ser DEFERIDA INTEGRALMENTE,** pelas razões e fundamentos expostos;

II - Seja reformada a decisão do Douto Pregoeiro Sr. Edilson Francisco Rodrigues, que declarou como vencedora a empresa **CLM Software Comercio Importação e Exportação Ltda**, **conforme motivos consignados neste RECURSO.**

III - Seja declarada vencedora do certame a empresa **Imagetech Tecnologia em Informática Ltda.**

IV - Caso o(a) Douto(a) Pregoeiro(a) opte por não aceitar o Recurso, **REQUEREMOS** que, com fulcro no Art. 9º da Lei 10.520/2002 C/C Art. 109, III, § 4º, da Lei 8666/93, e no princípio do duplo grau de jurisdição, seja remetido o processo para apreciação pela autoridade superior competente, para nova decisão, nos termos do aqui apresentado.

V - Requer, ainda, a produção de todo gênero de provas em direito admitidas na instrução do presente processo administrativo. E que seja enviado ao e-mail LICITACAO@GRUPOIMAGETECH.COM.BR Termos em que pede deferimento.

Campo Grande/MS 26 de maio de 2023

CELSO TADASHI TANAKA:[redacted]
DIRETORIA EXECUTIVA DE NEGOCIOS - GRUPO IMAGETECH
2023.05.26 14:44:47-04'00'

.....

Imagetech Tecnologia em Informática Ltda.
CNPJ 05.583.680/0001-37
Celso Tadashi Tanaka (Por procuração)
CPF [redacted]- RG [redacted]

ANEXO I

Relatório Ponto a Ponto

PROPOSTA TÉCNICA - PREGÃO 11/2023 - TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Especificações técnicas mínimas do Item 01	S	Comprovação Técnica	Link e Página
0. Especificações técnicas mínimas:			
1. Os appliances físicos devem ser novos e de primeiro uso;	S	Ciente e de acordo	Conforme proposta comercial
2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo servidor de uso genérico, e que atendam todas as funcionalidades descritas nas Especificações técnicas mínimas.	S	Ciente e de acordo	Conforme proposta comercial
3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie.	S	Ciente e de acordo	Conforme proposta comercial
4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-lido fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante.	S	Ciente e de acordo	Conforme proposta comercial
5. As funcionalidades da solução (balanceador de carga, global server load balancing, proteção para aplicação, proteção contataque DDoS, DNS Application Firewall, inspeção SSL etc) deverão ser licenciadas pelo período de 60 (sessenta) meses;	s	Ciente e de acordo	Conforme proposta comercial
6. O equipamento será instalado em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2Us dreferido rack;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
7. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos"), incluindo todos os cabos ligação lógica e elétrica necessários à instalação e perfeito funcionamento do equipamento no rack;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
8. Deve ser fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento.	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
9. Dispor de fonte de alimentação redundante com tensão de entrada de 110V a 220V AC automática e frequência de 60Hz;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
10. Possuir sistema operacional customizado especificamente para funções de Web Application Firewall, não podendo ser entregue appliance do tipo NGFW;	S	Página 3 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
11. Possuir, no mínimo, 06 interfaces, sendo 02 de 10GE com conectores padrão SFP+ (SR) e 04 portas SFP e transceivers (SR oUTP); Serão aceitas interfaces de maior capacidade, desde que possibilitem ser transformados em 10 GE (incluindo os cab"breakout" de, no mínimo, 3 metros);	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
12. Possuir 01 interfaces 1GE, incluso interfaces de gerência com conectores padrão RJ45;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
13. Todas as interfaces fornecidas devem estar licenciadas e habilitadas para uso imediato;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
14. Possuir no mínimo de 8.000 Mbps de throughput em camada 7;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
15. Possuir capacidade de 4.000 transações por segundo (TPS) em TLS padrão RSA (chaves de 2.048 bit). Serão aceitos equipamentos que apresentarem a mesma quantidade de conexões por segundo;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
16. Recursos de agregação de portas baseado no protocolo LACP, segundo o padrão IEEE 802.3ad;	S	Página 4 em Bonding, VLAN and VXLAN	https://kemptechnologies.com/files/packages/7.2.50.0.18765-RELEASE/docs/pdf/Feature_Description-Bonding_and_VLAN_and_VXLAN.pdf
17. Memória RAM mínima de 16 GB;	S	Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
18. Disco rígido com capacidade de armazenamento interno e retenção de logs para análise com capacidade mínima de 240GB;		Página 7 em Hardware Specifications	Página 7 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
19. Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;	S	Ciente e de acordo	Conforme proposta comercial
20. Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico;	S	Ciente e de acordo	Conforme proposta comercial
21. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração e hardware, para não onerar o sistema;	S	Página 3 em Hardware Specifications	Página 3 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
22. Suportar e garantir a instalação em ambiente de alta disponibilidade;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
23. Deve permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo ativo-ativo;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
24. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim permitir escalabilidade no futuro;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
25. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime " e queda de sessões ecaso de falha de uma das unidades;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
26. Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e persistência;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
27. O equipamento deve permitir a sincronização das configurações de forma automática;	S	Página Consta na Coluna seguinte	Página 6 do documento High Availability (HA) disponível emhttps://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-High_Availability_HA.pdf
28. Caso seja necessária uma interligação entre os equipamentos, a CONTRATADA será integralmente responsável por tinterligação, garantindo a performance necessária para o atendimento da solução;	S	Ciente e de acordo	Sim, atende conforme proposta comercial
29. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos SL GSLB,WAF, etc;	S	Ciente e de acordo	Sim, atende conforme proposta comercial
30. Fornecer recurso para o transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizandoprotocolo 802.1q;	S	Página 4 em Bonding, VLAN and VXLAN	Página 4 https://kemptechnologies.com/files/packages/7.2.50.0.18765-RELEASE/docs/pdf/Feature_Description-Bonding_and_VLAN_and_VXLAN.pdf
31. Analisar e proteger tráfego HTTP/1.0, HTTP/1.1, HTTP/2.0 e/ou HTTP/3;	S	Página Consta na Coluna seguinte	Página 10 Http no link https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-HTTP2.pdf
32. Possuir suporte a IPv6;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360004651751-IPV6-Configuration
33. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4IPv6,quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente cliente;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
34. Deve suportar, no mínimo, 1.000 VLANs simultaneamente;	S	Página 4 em Bonding, VLAN and VXLAN	Página 4 https://kemptechnologies.com/files/packages/7.2.50.0.18765-RELEASE/docs/pdf/Feature_Description-Bonding_and_VLAN_and_VXLAN.pdf
35. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360016052811-How-to-Configure-NTP
36. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software DefinNetwork);	S	Página 4 em Bonding, VLAN and VXLAN	Página 4 https://kemptechnologies.com/files/packages/7.2.50.0.18765-RELEASE/docs/pdf/Feature_Description-Bonding_and_VLAN_and_VXLAN.pdf
37. Assinar cookies digitalmente e editar endereços de URL ("URL Rewriting");	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/201836357-How-to-Modify-a-Root-URL-to-redirect-to-a-Specific-Directory-URL
38. O equipamento deverá permitir a sincronização das configurações:	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
a. De forma automática;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
b. Manualmente, forçando a sincronização apenas no momento desejado.	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
39. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
a. Compartilhar a rede de heartbeat com a rede de dados;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
b. Utilizar uma rede exclusiva para o heartbeat.	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
40. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfegoaumentar a proteção contra ataques;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
41. 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;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6440812670477-How-to-change-how-the-LM-syncs-across-units-in-an-HA-pair
42. Permitir a criação de políticas através de interface gráfica web ou CLI para manipulação de tráfego através de lógica para pemenos os seguintes operadores:	S	Página Consta na Coluna seguinte	Página 5 do documento https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Virtual_Services_and_Templates.pdf
Permitir a criação de políticas através de interface gráfica web ou CLI para manipulação de tráfego através de lógica para pemenos os seguintes operadores: a. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-urihttp-version	S	Página Consta na Coluna seguinte	Página 5 do documento https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Virtual_Services_and_Templates.pdf
43. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory o LDAP ou TACACS;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003655466-WUI-How-to-use-LDAP-for-WUI-Authentication
44. Deve implementar configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para a interface de gerenciamento;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/208670126-Interface-Description-Kemp-360-Central-Console-Administration-Interface
45. Permitir acesso in-band via SSH;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
46. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos: a. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs; b. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
a. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualizaçde configurações e logs;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
b. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
47. Manter internamente múltiplos arquivos de configurações do sistema;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
48. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
49. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ssuportados;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360014550212-How-to-create-a-Virtual-Service-for-Load-Balancing-LDAP-LDAPS-or-RADIUS-Requests
50. Deverá ser possível associar aos usuários de bases externas como RADIUS, LDAP e TACACS+ o nível de acesso;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360014550212-How-to-create-a-Virtual-Service-for-Load-Balancing-LDAP-LDAPS-or-RADIUS-Requests
51. Possuir Interface Gráfica via Web;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
52. Possuir auto-complementação de comandos na CLI;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941

Especificações técnicas mínimas do Item 01	S	Comprovação Técnica	Link e Página
53. Possuir ajuda contextual;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941
54. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas ou ter suporte a snmp v1/v2/v3 para monitoramendo equipamento;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202375677-LoadMaster-SNMP-MIBs-GA-LTSF-LTS-
a. A solução deve possuir arquivo de MIBS e documento descrevendo os OIDs e o que é possível coletar utilizando SNMP;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202375677-LoadMaster-SNMP-MIBs-GA-LTSF-LTS-
55. A Solução deve ter suporte a sFlow;	S	Página Consta na Coluna seguinte	Pagina 1 https://support.kemptechnologies.com/hc/en-us/articles/14337565569293
56. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941
57. Possuir, no mínimo, 3 (três) níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário SomenLeitura;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/10110114563341-User-Management
58. A interface gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso linha de comando;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/10110114563341-User-Management
59. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941
60. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941
61. Suportar a rollback de configuração salva e imagem;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
62. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
63. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
64. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
65. A interface Gráfica deverá permitir a reinicialização do equipamento;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/10686722539405-How-to-Reboot-the-LoadMaster
66. Reinicialização do equipamento por comando na CLI;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/14337564556941#MadCap_TOC_17_2
67. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/201121195-How-to-enable-SNMP-and-use-the-MIBs-for-Monitoring-the-LoadMaster
68. Possuir traps SNMP;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/201121195-How-to-enable-SNMP-and-use-the-MIBs-for-Monitoring-the-LoadMaster
69. Caso a solução possua suporte a RMON, deverá possuir suporte a monitoramento utilizando pelo menos 4 grupos:statistic history,alarms e events;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/201121195-How-to-enable-SNMP-and-use-the-MIBs-for-Monitoring-the-LoadMaster
70. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
71. Implementar Debugging : CLI via console e SSH;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/4423918508685-Extended-L7-Debug
72. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmendiferentes;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360014550212-How-to-create-a-Virtual-Service-for-Load-Balancing-LDAP-LDAPS-or-RADIUS-Requests
73. Permitir a criação de políticas diferenciadas por aplicação;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360014550212-How-to-create-a-Virtual-Service-for-Load-Balancing-LDAP-LDAPS-or-RADIUS-Requests
74. Deverá possuir uma funcionalidade de criação automática de políticas, para proteção DDoS e ataques zero-day onde a política segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/10110608498829-Web-Application-Firewall#MadCap_TOC_8_2
75. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/6514957861773-Content-Rules
76. Permitir as seguintes opções de implementação:	S		
a. Monitoramento (sem bloqueio);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Proxy (reverso e transparente).	S	Página Consta na Coluna seguinte	Pagina 5 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Transparency.pdf
77. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
78. Remover as mensagens de erro do conteúdo que será enviado aos usuários;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Technical_Note-WAF_Rule_Writing_Guide.pdf
79. Em modo "monitoramento" (sem bloqueio), realizar análise e avaliação do tráfego, gerar relatórios com os dados analisadossimular bloqueios para efeito de avaliação;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
80. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadoroperados por scripts ou qualquer outra forma que não operados por humanos;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
81. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
82. Possuir proteção para XML integrado com suporte a filtro e validação de funções XML específicas da aplicação, tais como, pexemplo: format check, limit check, sql injection check e cross-site scripting check;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
83. Com a finalidade de proteger as aplicações, a solução deve suportar proteções a JSON;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
84. Permitir a utilização de modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além proteção contra-ataques conhecidos aos protocolos HTTP e HTTPS;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
85. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
86. Bloqueio com intermediação e interrupção da conexão;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
87. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
88. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
89. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
90. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Endereços IP que originaram os ataques;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Horário do ataque;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
c. Nome do ataque;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
d. Qual campo foi atacado;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
e. Quantas vezes esse ataque foi realizado;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
91. possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
92. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
93. Identificar ataques baseados em:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Regras;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Perfis de utilização;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
c. Assinaturas e/ou comportamento.	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
94. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado;	S	Página Consta na Coluna seguinte	Página 52 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Product_Overview-Kemp_LoadMaster.pdf
95. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump permitindo uma análise mais aprofundada pparte do administrador;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360030802632-Performing-a-TCPDump
96. Detectar ataques de força bruta por meio dos seguintes métodos:	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
97. Aumento do tempo de resposta da aplicação monitorada ou bloqueio temporário do atacante;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
98. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
99. Detectar ataques do tipo força bruta em que:	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
a. O atacante solicita repetidamente o mesmo recurso;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
b. O atacante realiza repetidas tentativas não autorizadas de acesso;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
c. São utilizados ataques automatizados de login.	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
100. Detectar ataques do tipo força bruta que explorem:	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
a. Controles de acesso da aplicação (Erro 401 – Unauthorized);	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
b. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
c. Aplicações WEB que não retornam o Erro 401 (por meio da identificação de expressão regular no retorno/página de erro aplicação);	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
d. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de IPs);	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
e. Clientes automatizados (robôs, requisições muito rápidas);	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
f. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticatotalmente diferentes;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf

Especificações técnicas mínimas do Item 01	S	Comprovação Técnica	Link e Página
g. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
101. Apresentar proteção contra-ataques, como:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Brute Force Login ;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Buffer Overflow;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
c. Cookie Injection	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
d. Cookie Poisoning;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
e. Cross Site Request Forgery (CSRF);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
f. Cross Site Scripting (XSS);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
g. Server Side Request Forgery (SSRF)	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
h. Directory Traversal;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
i. HTTP Denial of Service ;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
j. Malicious Robots;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
k. Parameter Tampering	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
l. SQL Injection	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
m. Web Services (XML) attacks;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
102. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões protocolos, tipos de caracteres e versões utilizadas de cookies;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
103. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou macritérios simultaneamente:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Assinatura de ataque ou IPs de atacantes conhecidos;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Código de response ;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
c. Conteúdo da cookie ;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
d. Conteúdo do cabeçalho;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
e. Conteúdo do payload;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
f. Hostname ;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
g. IP de origem;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
h. Método HTTP;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
i. Número de ocorrências em determinado intervalo de tempo;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
j. Parâmetro;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
k. User-agent (navegador);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
104. Deve proteger contra os seguintes ataque:		Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Ataques de negação de serviços automatizados;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Worms e vulnerabilidades conhecidas;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
c. Requests em objetos restritos;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
105. Deve proteger contra ataques SSRF Server Side Request Forgery);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
106. A solução oferecida deverá possuir proteção contra ataques, disponibilizando acesso a base de assinaturas e/ou atualizaçõperiódicas até o fim do contrato;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
107. Ao atualizar ou adicionar uma nova configuração na política de proteção de WAF, a solução deve possuir opção de colocar a regou aplicação em modo " staging" ou " passive " para evitar falsos positivos e não bloquear tráfego válido;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
108. Deve permitir que possa ser especificado na política os tipos de arquivos que serão bloqueados (File Types);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
109. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação, ou enviar para inspeção através dprotocolo ICAP;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
110. Deve possuir uma proteção proativa comportamental contra ataques automatizados por robôs e outras ferramentas de ataque;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
111. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo repara proteção da aplicação;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
112. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manua	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
113. Possuir método de mitigação de DoS L7 baseado em:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Descarte de todas as requisições de um determinado IP e/ou país suspeito;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Defesa proativa contra Bot, através da injeção de um desafio no Browser ou via Javascript para detectar se é um usuárlegítimo ou robô;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
114. Aprender o comportamento da aplicação:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Campos, valores e URLs;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
115. Políticas sugeridas somente devem ser aplicadas após um período configurável ou possibilidade de aplicá-las posteriormente;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
116. Inspecionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formuláriosconteúdo, além de inspecionar os requests e responses;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
117. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies , campos ocultos e parâmetroconsultas (query), métodos HTTP, elementos XML e ações SOAP;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
118. Proteger contra mensagens XML e SOAP malformadas;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
119. Utilizar o campo HTTP X-Forwarded - For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes coNAT;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
120. Remover as mensagens de erro do conteúdo que será enviado aos usuários;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
121. Deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática ou vir com lista dos principarobôs já pré-configurada, inclusive para Robôs conhecidos do mercado, como por exemplo Google, Yahoo e Microsoft Bing, qudeverão ser liberados por padrão;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
122. Deverá permitir o cadastro de robôs que podem acessar a aplicação;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
123. Deverá implementar proteção ao JSON (JavaScript Object Notation);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
124. Deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritaEste bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
125. Deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicação. Essas informaçõdevem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da aplicação;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
126. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados. Deve protegesses dados criptografados de malwares e keyloggers;	s	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
127. Deve ofuscar o nome de um parâmetro sensível da aplicação em caracteres randômicos. Esse nome de parâmetro deve ser mudadconstantemente pela ferramenta para dificultar ataques direcionados;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
128. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques Robôs, Violações, URL, Endereços IP, Países, Severidade.	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
129. Deverá permitir o agendamento de relatórios a serem entregues por e-mail;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
130. Emitir os seguintes relatórios gráficos dos ataques por:	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
a. Política de segurança;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
b. Tipos de ataques;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf

Especificações técnicas mínimas do Item 01	S	Comprovação Técnica	Link e Página
c. Violações;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
d. URL que foram atacadas;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
e. Endereços IP de origem;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
f. Localização geográfica dos endereços IPs de origem;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
g. Severidade;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
h. Código de resposta;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
i. Métodos;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
j. Protocolos;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
k. Sessão;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
131. Permitir a seleção de período para emissão dos relatórios;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
132. Permitir a geração das seguintes informações, por período:	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
a. Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;	S	Página Consta na Coluna seguinte	Página 1 https://kemptechnologies.com/kemp360/configuration-management
b. Informações estatísticas de quantidade de conexões completadas e bloqueadas;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
c. Informações estatísticas de fluxo de tráfego;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
133. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS;	S	Página Consta na Coluna seguinte	Página 1 https://kemptechnologies.com/es/faq/general/how-can-i-redirect-traffic-http-https
134. Deve possuir capacidade para definir que todo tráfego seja tunelado e permitir a utilização do protocolo padrão HTTPS com SScomo transporte, possibilitando a sua utilização com proxy HTTP e possibilitar utilização de encapsulamento;	S	Página Consta na Coluna seguinte	Página 1 https://kemptechnologies.com/es/faq/general/how-can-i-redirect-traffic-http-https
135. Deve possuir capacidade para definir servidor virtual em HTTPS com perfil cliente SSL/TLS padrão e redirecionar tráfego HTTpara HTTPS para um determinado servidor virtual;	S	Página Consta na Coluna seguinte	Página 1 https://kemptechnologies.com/es/faq/general/how-can-i-redirect-traffic-http-https
136. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidopodendo assim operar em modo "man in the middle", ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL/TLS secomprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor;	s	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
137. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo demais otimizações em ambiente 100% criptografado;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
138. A solução deve possuir recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto nperformance das aplicações. Dentre eles deve ser possível configurar parâmetros como:	S		
a. SSLsession cache timeout;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
b. Session ticket;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
c. OCSP (Online Certificate Status Protocol)Stapling;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
d. Perfect forward secrecy;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
139. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas nesse edital devem estar disponíveis quando a conexão segura for estabelecida usando:	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
a. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo ladservidor durante o processo de estabelecimento do túnel SSL/TLS;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
b. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecidpelo cliente durante o processo de estabelecimento do túnel SSL/TLS;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
c. Ao realizar inspeção, proteção,offload e aceleração de tráfego criptografado através de SSL/TLS;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
d. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo ladcliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/115003853166-How-To-Import-SSL-Certificates-To-Your-LoadMaster
140. Deve possibilitar a customização da interface gráfica da página de login;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
141. A solução deve oferecer ferramenta de Portal de Acesso de Usuários que permita que usuários acessem aplicações internas a parde rede externas, implementando as funcionalidades de Single Sign-one/ou VPN-SSL, com,pelo menos, os seguintes recurspara cada funcionalidade:	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
a. Single Sign-on	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
i. modo "Portal" onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internos apresentando-os como links seguros no portal do usuário;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
ii. Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais qurequeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
b. VPN-SSL:	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
i. modo "Túnel por aplicação" onde o usuário estabelece túnel somente para o tráfego da aplicação, não sendo permitidoutro tipo de tráfego dentro do mesmo túnel;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
ii. rtal" onde o equipamento se comporta como proxy reverso, buscando o conteúdo Web dos portais internosapresentando-os como links seguros no portal do usuário;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
iii. modo "Network", onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela reinterna;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
iv. Ser capaz de solicitar as credenciais do usuário somente uma vez, e autenticar o usuário em todos os portais qurequeiram autenticação, fazendo cache das credenciais do usuário e utilizar a credencial correta para cada sistema;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
v. Deverá ser compatível para Microsoft Windows, Linux, dispositivos/ baseados em Android e iOS e MAC OSX;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
c. Para a ferramenta de Portal de Acesso de Usuários, deverá ser capaz de autenticar usuários em bases de dados, como pexemplo: LDAP, Radius, Tacacs+, Kerberos e RSA SecurID;	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
142. Deve suportar autenticação de múltiplos fatores utilizando tokens de Hardware ou One-Time Passcode (OTP);	S	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Edge_Security_Pack_ESP.pdf
143. Deve possuir capacidade para realizar proxy reverso com a finalidade de omitir a URI real, promovendo assim o acesso seguro aplicações web internas;	S	Página 4 em Hardware Specifications	Página 4 em Hardware Specifications https://kemptechnologies.com/docs/kemptechnologieslibraries/loadmaster/loadmaster-hw.pdf
144. Melhora da disponibilidade das aplicações através do balanceamento da entrada de tráfego deve possuir, ao menos, as seguintcaracterísticas:	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
a. DNS autoritativo;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
b. DNS secundário;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
c. DNS resolver;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
d. DNS cache;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
e. Balanceamento de DNS servers;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
f. DNSSec;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
145. Capacidade de uso de chave criptográfica para comunicação segura entre servidores DNS, obedecendo no mínimo os padrõe HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
146. A solução deve realizar offload dos servidores de DNS, funcionando como o DNS secundário;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
147. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, MX,NS, PTR, SRV, TXT;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
148. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: aplicação, nome daquery , tipo da query, endereço IP do cliente;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
149. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudançna infraestrutura;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
150. Deve prover as respostas a queries DNS da própria RAM CACHE;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
151. A solução deve ser capaz de realizar IP Anycast;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
152. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
153. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento;	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
154. A solução deve suportar, no mínimo, os seguintes métodos de balanceamento:			
a. Round Robin	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202017723-KEMP-LoadMaster-Scheduling-Balancing-Methods
b. Global Availability;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202017723-KEMP-LoadMaster-Scheduling-Balancing-Methods
c. Geografia;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202017723-KEMP-LoadMaster-Scheduling-Balancing-Methods
d. Least Connections;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202017723-KEMP-LoadMaster-Scheduling-Balancing-Methods
155. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);	S	Página Consta na Coluna seguinte	Página 7 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf

Especificações técnicas mínimas do Item 01	S	Comprovação Técnica	Link e Página
156. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes ou encaminhar requisições clientes (screening);	S	Página Consta na Coluna seguinte	Página 53 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-GEO.pdf
157. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360002990271-How-to-understand-configure-Caching
158. Possuir no mínimo um dos tipo de compressão a seguir: gzip1 a gzip9 ou deflate;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360002990271-How-to-understand-configure-Caching
159. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360002990271-How-to-understand-configure-Caching
160. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo aplicação;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360002990271-How-to-understand-configure-Caching
161. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;	s	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360002990271-How-to-understand-configure-Caching
162. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistêncde sessão dos seguintes tipos:	s		
a. Por cookie;	s	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202040875
b. Endereço de origem;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202040875
c. Sessão SSL;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202040875
d. Através de qualquer parâmetro do cabeçalho HTTP;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202040875
e. Através da análise do SIP Call ID ou Source IP;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/202040875
163. O equipamento oferecido deverá possuir monitores predefinidos ou possibilitar a configuração para, no mínimo, os seguintes protocolos:			
a. ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP, IMAP, SMTPOP3, SIP, Real Server, SOAP, SNMP e WMI;	s	Página Consta na Coluna seguinte	Página 6 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Health_Checking.pdf
164. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
165. RealizarNetwork Address Translation(NAT);	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
166. Realizar proteção contrasyn flood;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
167. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content- Type- Options;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
168. Permitir espelhamento do trafego, de forma que a solução envie uma cópia do tráfego para um analisador, como por exemplo u poolde IDSs ouSniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidou indicações de atividade maliciosas ou ataques de rede;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
169. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
a. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução de automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
b. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deautomaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original;	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
170. Possuir capacidae de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientnestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço	s	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
171. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
172. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
173. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
174. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;	S	Página Consta na Coluna seguinte	Página 9 https://kemptechnologies.com/files/packages/7.2.58.0.21782-RELEASE/docs/pdf/Feature_Description-Rate_Limiting.pdf
175. RealizarNetwork Address Translation (NAT);	s	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/201489169-How-to-configure-Kemp-LoadMaster-Use-Address-for-Server-NAT
176. Realizar proteção contra Denial of Service (DoS);	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
177. Realizar proteção contra Syn flood ;	s	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
178. Realizar limpeza de cabeçalho HTTP;	S	Página Consta na Coluna seguinte	Página 13 https://kemptechnologies.com/files/packages/7.2.59.0.22007-RELEASE/docs/pdf/Feature_Description-Web_Application_Firewall.pdf
179. Deve possuir suporte a Link Layer Discovery Protocol (LLDP);	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/200932505-How-to-Configure-VLAN-s-on-Kemp-LoadMaster
180. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
181. Deve ser capaz de realizar DHCP relay;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
182. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
a. Tempo de resposta da aplicação;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
b. Latência;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
c. Conexões para cnjunto de servidores, servidores individuais;	s	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
d. Por URL;	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360003151512-How-to-view-the-LoadMaster-s-Metrics-and-Connection-Statistics
e. A solução deve ter suporte a TLS 1.3.	S	Página Consta na Coluna seguinte	Página 1 https://support.kemptechnologies.com/hc/en-us/articles/360021824851-LoadMaster-7-2-45-0-Release-Notes

Especificações técnicas mínimas do Item 01	S
Especificações técnicas mínimas do Item 02	Ciente e de acordo
1. Os serviços de instalação física, lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fasesseguir.	Ciente e de acordo
2. Fase de abertura:	Ciente e de acordo
a. Validar e Homologar escopo do projeto;	Ciente e de acordo
b. Validar objetivos e premissas do projeto;	Ciente e de acordo
c. Validar riscos e restrições do projeto;	Ciente e de acordo
d. Identificar e validar os requisitos do projeto;	Ciente e de acordo
e. Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informaçõapresentado nesta especificação técnica;	Ciente e de acordo
f. Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;	Ciente e de acordo
g. Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.	Ciente e de acordo
3. Fase de planejamento:	Ciente e de acordo
a. Elaborar plano de projeto;	Ciente e de acordo
b. Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;	Ciente e de acordo
c. Reunir as equipes da CONTRATADA e CONTRATANTE;	Ciente e de acordo
d. Definir os arâmetros de configuração básicos e avançados a serem implementados;	Ciente e de acordo
e. Apresentar o Mapa de rede contendo a topologia a ser implementada;	Ciente e de acordo
f. Apresentação do cronograma do projeto com os prazos e responsabilidades;	Ciente e de acordo
g. Verificar os pré-requisitos do projeto;	Ciente e de acordo
h. Apresentar plano do projeto para a homologação por parte da CONTRATANTE.	Ciente e de acordo
4. Fase de execução: O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidacom o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ambiente de infraestrutura de informática da CONTRATANTE e deve contemplar, no mínimo, o seguinte:	Ciente e de acordo
a. Deverão ser realizados por conta da contratada o armazenamento, a embalagem, o transporte, a entrega e a instalação todo e qualquer item do objeto do edital, de tal maneira que a contratada será responsável pela remessa de todos equipamentos para o(s) endereços informados no Edital, nos quais a solução de segurança será efetivamente implantada.	Ciente e de acordo
b. A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabrican(recommended settings);	Ciente e de acordo
c. A CONTRATADA deverá efetuar a instalação do appliance virtual ou físico (conforme item solicitado) na infraestrutuindicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações dfabricante (recommended settings);	Ciente e de acordo
d. Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusiconfiguração de VLANs e interfaces virtuais, se for o caso;	Ciente e de acordo
e. Atualização de softwares, firmwares e drivers que compõem a solução;	Ciente e de acordo
f. A CONTRATADA deverá fornecer, quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexpara interligar fisicamente todos os componentes da solução entregue;	Ciente e de acordo
g. Aplicação das licenças necessárias à solução entregue;	Ciente e de acordo
h. Testes da solução, incluindo testes de failover;	Ciente e de acordo
i. Documentação do ambiente configurado e instalado;	Ciente e de acordo
5. os de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em semanuais de instalação e configuração ou artigos técnicos.	Ciente e de acordo
6. A solução, deverá ser entregue com todas as funcionalidades, recursos, componentes, acessórios, softwares e licenciamentnecessários ao seu pleno funcionamento.	Ciente e de acordo
7. Todas as informações necessárias à implantação, como topologia de rede, VLANs, endereçamento IP, portas de Swtichs que deveser utilizadas e outras necessárias à perfeita configuração, interligação e funcionamento da solução serão fornecidas peCONTRATANTE.	Ciente e de acordo
8. A instalação da solução, incluindo todos os componentes e acessórios, será realizada pela CONTRATADA, com acompanhamende uma equipe destacada pela CONTRATANTE.	Ciente e de acordo
9. A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade instalação e a configuração dos equipamentos e softwares que compõem a solução.	Ciente e de acordo
10. A instalação, configuração e testes do equipamento deverá ser feita com o acompanhamento de técnicos da CONTRATANTvisando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança da CONTRATANTE.	Ciente e de acordo
11. A CONTRATADA deverá efetuar a instalação/configuração conforme a definição da arquitetura de cada sistema, envolvendo pemenos:	Ciente e de acordo
a. O agrupamento dos "appliances" em configuração do tipo "cluster" do tipo ativo/ativo ou ativo/passivo;	Ciente e de acordo
b. Segmentação das redes por meio do uso de VLANs;	Ciente e de acordo
c. Definição das redes IP a serem empregadas pelos servidores reais (redes de serviço);	Ciente e de acordo
d. A criação de usuários para fins de operação e administração do sistema.	Ciente e de acordo
e. Configuação de alarmes e notificações automatizadas a serem enviadas via protocolos SNMP e/ou SMTP.	Ciente e de acordo
f. Configuração da topologia de conectividade de rede entre o sistema e os ativos de rede em operação nos datacenters dcontratante	Ciente e de acordo
g. Instalação, registro e ativação de licenças para todos os equipamentos ofertados, em total conformidade com esespecificação técnica.	Ciente e de acordo
h. Teste e homologação do conjunto de recursos e funcionalidades do sistema implantado.	Ciente e de acordo

Especificações técnicas mínimas do Item 01	S
12. A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriadsem custo adicional para o contratante, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dserviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dequipamentos poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade ou quvenham a requerer a parada dos equipamentos deverão ser executadas fora do horário de expediente, inclusive em feriados ofinais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE.	Ciente e de acordo
a. Atividades associadas à implantação com a necessidade de interrupção de serviços em produção, deverão ocorrer fora dexpediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANT	Ciente e de acordo
13. O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 30(trinta) dias, contados a partir confirmação do recebimento da Ordem de Serviço.	Ciente e de acordo
a. Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em plenfuncionamento, incluindo documentação "As Built", contendo planejamento, relatório de instalação, configuração adotadtestes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidnesta especificação técnica.	Ciente e de acordo
14. Características do repasse de conhecimento hands-on:	Ciente e de acordo
a. Efetuar o repasse hands-on com carga horária de, no mínimo, 6 (seis) horas para o repasse de conhecimento referenteintegração da solução e sua implantação com a transferência das informações básicas de configuração e operação;	Ciente e de acordo
b. O repasse de informações deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimizaçãresolução de problemas e utilização da solução;	Ciente e de acordo
c. A equipe técnica do Tribunal, responsável pela infraestrutura técnica deverá disponibilizar no mínimo 2(dois) e no máxim6(seis)técnicos para o acompanhamento das atividades de hands-on.	Ciente e de acordo
15. horas do acompanhamento hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades instalação/configuração, mediante proposição da equipe técnica do Tribunal, com a anuência da fiscalização do Contrato.	Ciente e de acordo
16. Condições de aceitação do repasse hands-on	Ciente e de acordo
a. Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar na prática funcionalidades principais da solução WAF, particularmente, as atividades relacionadas à mudança de configuração operação da solução.	Ciente e de acordo
b. A não aceitação do hands-on implicará a na não aceitação da entrega definitiva do serviço (ITEM 4).	Ciente e de acordo
c. Todas as despesas de instrutor(es), deslocamento de instrutor(es) e demais itens relacionados ao repasse Hands-On, serão responsabilidade da CONTRATADA.	Ciente e de acordo
	Ciente e de acordo
Especificações técnicas mínimas do Item 03	Ciente e de acordo
	Ciente e de acordo
1. Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher	Ciente e de acordo
para treinamento, cujo escopo dtreinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares eprodução, bem como planejar mudanças de configuração no ambiente:	Ciente e de acordo
a. O treinamento deverá oferecer carga horária total de no mínimo 20 (vinte) horas;	Ciente e de acordo
b. Serão aceitos preferencialmente treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online vivo serem gravados, a critério da CONTRATANTE;	Ciente e de acordo
c. A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes	Ciente e de acordo
d. Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia;	Ciente e de acordo
e. O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimizaçãresolução de problemas e utilização da solução.	Ciente e de acordo
2. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA;	Ciente e de acordo
3. O treinamento poderá ser composto de mais de 1 (um) módulo, que deverão ser discriminados na proposta da licitante;	Ciente e de acordo
4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar quo(s)treinamento(s) ofertados cobrem os conhecimentos necessários para instalação, administração, configuração, gerênciotimização, resolução de problemas e utilização da solução;	Ciente e de acordo
	Ciente e de acordo
5. O Tribunal poderá planejar e escolher quaisquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata registro de preços, a contar da entrega do calendário;	Ciente e de acordo
6. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dequipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada;	Ciente e de acordo
7. É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável peatendimento do contratado para todos os fins;	Ciente e de acordo
8. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada nassinatura do Contrato;	Ciente e de acordo
9. A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português;	Ciente e de acordo
10. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, seaceito material em inglês.	Ciente e de acordo

Especificações técnicas mínimas do Item 01	S
11. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução exercícios práticos.	Ciente e de acordo
a. No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratóriotodos os produtos ofertados (ou similares) para realização da capacitação;	Ciente e de acordo
12. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteapós o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carhorária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento;	Ciente e de acordo
13 .A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo à contratada informar no certificado a carhorária e assiduidade do servidor	Ciente e de acordo
14. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo Referência.	Ciente e de acordo
a. No Formulário, será utilizada escala de até 4 (quatro) pontos para cada quesito do formulário. No mínimo 70% dparticipantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.	Ciente e de acordo
b. O resultado da Avaliação de Instrutor será utilizado como critério de aceitação do treinamento, devendo ser considerado peamostra de participantes como “proveitoso” para no mínimo 04(quatro) dos 07(sete) itens avaliados;	Ciente e de acordo
c. Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado naceito;	Ciente e de acordo
d. Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outinstrutor, sem qualquer ônus para o CONTRATANTE;	Ciente e de acordo
e. Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-as sanções previstas contratualmente.	Ciente e de acordo
	Ciente e de acordo
Especificações técnicas mínimas do Item 04	Ciente e de acordo
	Ciente e de acordo
1. Crédito de horas técnicas para a prestação de serviços de suporte especializado e consultoria, após a conclusão da instalaçãconfiguração e treinamento da solução ofertada;	Ciente e de acordo
2. Os serviços de suporte especializado e consultoria deverão abranger, mas não se limitando, a demandas de administração, operaçassistida, planejamento e tuning, detecção e correção de erros, apoio à operação, análise de desempenho, ajustes, recomendação boas práticas, reconfiguração e integração com outros sistemas do ambiente da CONTRATANTE;	Ciente e de acordo
3. O banco de horas técnicas poderá ser utilizado em até 12 (doze) meses e deverá ter tempo de resposta de até 04 (quatro) horas;	Ciente e de acordo
4. As horas técnicas poderão ser utilizadas em dias consecutivos ou alternados e serão contabilizados em termos de homem/hora;	Ciente e de acordo
5. As horas técnicas serão consumidas sob demanda, de acordo com as necessidades da CONTRATANTE;	Ciente e de acordo
6. Os serviços técnicos especializados poderão ser executados presencial ou remotamente;	Ciente e de acordo
7. Para a execução dos serviços técnicos especializados, a CONTRATANTE elaborará documento de escopo do serviço a srealizado com as entregas que deverão ser alcançadas e, em comum acordo com a CONTRATADA, definirá a quantidade de horestimadas, os prazos de execução com datas de início e encerramento do atendimento;	Ciente e de acordo
8. Qualquer alteração na quantidade de horas previstas para a realização da demanda deverá ser justificada e previamente aprovapela CONTRATANTE;	Ciente e de acordo
9. Os serviços serão realizados utilizando o regime de 8x5 para atendimentos programados. Para atendimentos emergenciais e fora dhorário comercial, em regime 24x7, serão computadas horas em dobro;	Ciente e de acordo
10. A CONTRATADA deverá produzir, como resultado de cada atendimento técnico realizado, um Relatório de Atendimento Técni- RAT, contendo no mínimo as seguintes informações:	Ciente e de acordo
a. Discriminação das atividades executadas;	Ciente e de acordo
b. Resultados obtidos;	Ciente e de acordo
c. Conclusões técnicas e sugestões para melhoria do ambiente;	Ciente e de acordo
d. Total de horas utilizadas, contendo o início, interrupções e final do atendimento	Ciente e de acordo
11. A CONTRATADA deverá entregar o RAT à CONTRATANTE, no prazo máximo de 2 (dois) dias úteis, após a conclusão dserviços;	Ciente e de acordo
12. O serviço será considerado concluído após o aceite da CONTRATANTE;	Ciente e de acordo
13. A CONTRATANTE emitirá aceite de prestação de suporte técnico, após a conclusão do serviço, condicionado à verificação conformidade do serviço executado;	Ciente e de acordo
14. O faturamento dos serviços técnicos utilizados será realizado mensalmente e considerará os chamados abertos e concluídos dentdo mês de referência.	Ciente e de acordo

ANEXO II

Conformidade com a RoHS

Kemp Technologies, Política Ambiental RoHS

Como cidadão global para a construção de infraestrutura digital, a Kemp está comprometida com produtos ecológicos em conformidade com todos os requisitos estatutários e regulamentares ambientais relevantes para ser seu parceiro ecológico confiável e ajudar a proteger nosso meio ambiente.

A Kemp se compromete a fornecer apenas produtos que estejam em conformidade com as Diretivas RoHS da União Europeia 2011/65/EU e UE 2015/863.

A diretiva RoHS 1 – Restrição do uso de certas substâncias perigosas em equipamentos elétricos e eletrônicos (EEE) – (2002/95/CE) se aplica a certas categorias de EEE desde 1º de julho de 2006. A nova diretiva RoHS 2 revisada (2011/ 65/EU) substituiu a RoHS 1 em 2 de janeiro de 2013 e a nova diretiva RoHS 3 alterará a diretiva RoHS 2 para adicionar 4 substâncias restritas adicionais às 6 já mencionadas.

As substâncias às quais se aplica a diretiva RoHS 1 (RoHS 2 e RoHS 3) são (incluindo os valores máximos de concentração por peso em materiais homogêneos):

- Chumbo (Pb) - 0,1%
- Mercúrio (Hg) - 0,1%
- Bifenis polibromados (PBB) - 0,1%
- Cromo hexavalente (Cr(VI)) - 0,1%
- Cádmio (Cd) - 0,01%
- Éteres difenílicos polibromados (PBDE) - 0,1%
- Bis(2-etilhexil)ftalato (DEHP) - 0,1%
- Butil benzil ftalato (BBP) - 0,1%
- Dibutil ftalato (DBP) - 0,1%
- Diisobutil ftalato (DIBP) - 0,1%

O hardware da Kemp não excede (em peso) os níveis de concentração das substâncias acima.

De acordo com a diretiva RoHS, os 'produtores' de equipamentos são responsáveis por garantir que seus produtos não contenham nenhuma das 10 substâncias restritas. Um 'produtor' é definido como qualquer pessoa/organização que:

1. fabrica e comercializa equipamentos eletroeletrônicos com marca própria;
2. revende com marca própria equipamentos produzidos por outros fornecedores; ou
3. importa ou exporta equipamento elétrico e eletrônico profissionalmente para um estado membro.

De acordo com a RoHS 1, não há nenhum requisito específico sobre como os produtos serão identificados como compatíveis com a RoHS. Muitos produtores adotaram seus próprios logotipos com a Kemp usando os seguintes logotipos em nosso produto padrão, quando aplicável:

Conformidade política

Política RoHS

Política WEEE

Política REACH

lixo eletrônico

Conformidade de exportação

Conformidade com Código de Terceiros

Produto, suporte e serviços

Ligue para casa

Termos de Serviço da Assinatura de Suporte

Política de Autorização de Devolução de Material

Contrato de licença do usuário final

Privacidade

Centro de privacidade de progresso

Kemp Analytics

Organizacional

Certificação ISO

Política de qualidade

Declaração de Gestão da Qualidade

Resposta ao Coronavirus

Conformidade de exportação

RoHS 2 é uma diretiva de marcação CE que é aplicada na União Europeia a partir de 2 de janeiro de 2013.

A marcação Avaliação de Conformidade do Reino Unido (UKCA) é uma diretiva de marcação do Reino Unido a partir de 1º de janeiro de 2021.

Todos os produtos dentro do escopo das diretivas de marcação CE e UKCA devem atender aos seguintes requisitos:

- Produtos acabados com marca CE ou UKCA
- Declarações de Conformidade (D de C) para incluir a diretiva RoHS
- Documentação técnica deve ser mantida por 10 anos

Este requisito afeta fabricantes, importadores e distribuidores e significa que toda a cadeia de suprimentos da UE ou do Reino Unido tem responsabilidade legal pela conformidade.

- Como fabricante, a Kemp tem a responsabilidade de concluir as seguintes atividades para todos os produtos dentro do escopo:
- Compilar a documentação técnica
- Prepare as Declarações de Conformidade relevantes
- CE ou UKCA marcam os produtos
- Marcar produtos para rastreabilidade
- Guarde a documentação técnica por 10 anos
- Trabalhar com as autoridades nacionais para demonstrar conformidade ou ajudar a garantir a conformidade

Se você precisar de mais informações sobre o compromisso da Kemps com a RoHS, entre em contato com compliance@kemp.ax .

Assinado:

Iain Kenney
Vice-presidente de gerenciamento de produtos
ikenney@kemptechnologies.com
Kemp Technologies