OFÍCIO N. 176/2026
ASSUNTO: Pedido de esclarecimentos ao Edital do PE nº. 032/2026.
PROCESSO N. 8515550-95.2025.8.06.0000

Fortaleza, 03 de setembro de 2026.

Prezado (s) Senhor (es),

Em resposta ao questionamento enviado ao endereço eletrônico da Comissão Permanente de Contratação do TJCE, em 01/09/2026 às 17:41h, por empresa interessada em participar do Pregão Eletrônico n. 032/2026, informo os esclarecimentos, que seguem:

Pergunta 1:

"1 – 1. VOLUME DE REQUISIÇÕES
Observamos que o edital não adota a quantidade de requisições como critério de cobrança ou limitação contratual, conforme itens 1.3.6 e 1.3.8 do Anexo II. Contudo, o conhecimento desses números é pré-requisito para nossa precificação de arquitetura e tem o objetivo de assegurar a melhor experiência de performance e segurança desde o início da operação.
Com o objetivo de aprimorar o dimensionamento técnico da solução e garantir a adequada alocação de recursos, solicitamos, a título de referência, a informação sobre o volume médio e de pico mensal de requisições atualmente observado nas aplicações que serão protegidas.

Resposta 1:

O entendimento está correto: requisições, conexões, sessões ou chamadas de API não constituem métrica de cobrança, licenciamento ou limitação (Anexo II, itens 1.3.6 e 2.1.10).
O TJCE não dispõe de métrica de requisições no perímetro do WAF. O Estudo Técnico Preliminar registra a limitação no item 8.5.3.1, e os valores de RPS do item 1.1.4.4 decorrem da medição dos appliances NetScaler (item 5.3.2.2), que processa o tráfego da rede interno, não direcionado à internet pública e insuscetível de tratamento por solução em nuvem (item 4.2.1).
A volumetria disponível para o Lote 2 é a da seção 8.5 do ETP: média de 1,67 TB/dia, cerca de 50 TB/mês, apurada no firewall de borda em 90 dias, restrita a aplicações SSL/Web Browsing da zona de internet (item 8.5.1), e picos de aproximadamente 500 Mbps na interface da DMZ (item 8.5.2). O dado é informativo e não vincula a Administração.
Os parâmetros de dimensionamento são os do Anexo II: franquia mensal mínima de 50 TB e banda mínima de 1 Gbps (item 1.3.5), franquia adicional sob demanda, sem compromisso mínimo de consumo (item 2.1.5), e no mínimo 255 FQDNs (item 1.4.15). O dimensionamento da arquitetura ofertada compete à licitante, cujas especificações vinculam a proposta (item 4.3.5 do Edital), devendo absorver picos legítimos de tráfego sem ajustes emergenciais ou licenças adicionais (item 1.3.8).

Pergunta 2:

"2 – DIMENSIONAMENTO DE LOAD BALANCING E GSLB

O Anexo II, item 1.4.25.3, estabelece que a solução deverá suportar configuração de múltiplos servidores de origem em pelo menos 2 links de internet, com failover automático.
O Estudo Técnico Preliminar, item 8.5.4, menciona que a plataforma de DNS em nuvem deve implementar configuração de até 320 registros de DNS para funcionalidade de balanceamento de sites (GSLB).
Contudo, o edital não detalha quantos pools, origins, monitores de saúde e decisões de GSLB serão efetivamente necessários. Nesse contexto, para o correto dimensionamento da arquitetura, solicitamos as seguintes informações complementares:
a. Além da arquitetura mínima com duas origens, quantos pools (grupos de servidores) e origins (servidores de origem) devem ser configurados?
b. Quantos monitores de saúde (health checks) serão necessários por pool ou origem?
c. A funcionalidade de GSLB deverá abranger todos os 320 registros de DNS mencionados no ETP ou apenas um subconjunto?

Resposta 2:

Preliminarmente, o item 8.5.4 do ETP não trata de registros de DNS para GSLB: refere-se aos 255 FQDNs vinculados a uma única zona DNS institucional. A exigência de até 320 registros consta do Anexo II, item 3.8.3.
(a) e (b) O Anexo II não fixa quantidade de pools, origens ou monitores de saúde. Os itens 1.4.25.1 a 1.4.25.3 estabelecem requisito funcional da plataforma, aplicável aos FQDNs protegidos na forma do item 1.4.15. A definição de quais FQDNs utilizarão a funcionalidade e seu agrupamento ocorrerá na fase de implantação (itens 1.9.10 e 1.9.11), estando os custos correspondentes inclusos no preço proposto (item 4.3.6 do Edital).
(c) A solução deverá suportar a configuração de até 320 registros de DNS para GSLB (item 3.8.3), capacidade mínima da plataforma disponível desde a contratação. A quantidade efetivamente configurada será definida na implantação, dentro desse limite.

Pergunta 3:

"3 – ENDPOINTS DE API A SEREM PROTEGIDOS
O Anexo II, item 1.7, estabelece requisitos para a proteção de APIs, incluindo descoberta automática de endpoints (item 1.7.9), proteção contra "Shadow APIs" (item 1.7.13) e validação de autenticação via mTLS (item 1.7.11).
a. Qual é a quantidade estimada ou máxima de endpoints de API que deverão ser protegidos pela solução?
b. Fica claro que todas as funcionalidades de proteção e controle de APIs autenticação mTLS devem estar plenamente licenciadas e prontas para o uso deste tribunal, correto?
O Anexo II, item 1.4.57.1, exige que a solução exponha "API REST autenticada para consulta e alteração de configurações de segurança e CDN, com autenticação baseada em tokens ou certificados, suportando Mutual TLS (mTLS) para chamadas automatizadas.
a. Podemos considerar também neste caso o uso de mTLS para autenticação em tokens ou certificados deve estar totalmente licenciada, correto?

Resposta 3:

(a) O Anexo II não fixa quantidade de endpoints de API. O escopo alcança as APIs associadas aos sites protegidos (item 1.7.4), limitado às aplicações publicadas sob os FQDNs do item 1.4.15, cabendo à solução a identificação dos endpoints por descoberta automática, inclusive dos não declarados (itens 1.7.9 e 1.7.13). É vedada limitação técnica ou comercial baseada em chamadas de API ou métricas equivalentes, inclusive por quantidade de endpoints (item 1.3.6).
(b) O entendimento está correto quanto à disponibilidade das funcionalidades. A validação de autenticação via mTLS na API (item 1.7.11) e o suporte a mTLS para aplicações web e APIs, com lista de Autoridades Certificadoras de confiança e verificação em listas de revogação (item 1.4.24.9), deverão estar homologados e disponíveis para uso em produção no momento da contratação (item 1.3.4). O mesmo se aplica à API REST de gerenciamento (item 1.4.57.1), sem custo adicional (item 4.3.6 do Edital). O Anexo II não exige da CONTRATADA a emissão ou a gestão de certificados de cliente, limitando-se à sua validação.

Pergunta 4:

“**4 – ARQUITETURA DE MITIGAÇÃO DDoS E DO "SCRUBBING CENTER"**
O Anexo II, item 1.4.1, estabelece que a CDN deve possuir capacidade de mitigação "descentralizada e independente, com todas as funcionalidades de proteção (sem a necessidade de desvio de tráfego para um 'scrubbing center') ".
a. Qual o critério objetivo que será adotado pela Comissão para comprovar que a solução ofertada não depende de desvio de tráfego para um "scrubbing center", conforme vedação expressa no item 1.4.1?
b. Será exigida, para fins de comprovação, declaração formal do fabricante atestando que sua arquitetura de mitigação DDoS é integralmente distribuída e não utiliza "scrubbing centers" centralizados para processamento do tráfego?
c. Entendemos assim que qualquer tipo de arquitetura que use "scrubbing centers", está completamente proibida, correto?

Resposta 4:

(a) O critério é o texto dos itens 1.4.1 e 1.4.28. A verificação ocorre na fase de aceitação e julgamento da proposta (item 4.9.4 do Edital), com base na documentação técnica oficial do fabricante da solução ofertada, que a licitante poderá anexar à proposta na forma do item 4.3.4.1, observada a vedação de identificação, sob pena de desclassificação por desatendimento das especificações técnicas (item 4.10.8.2). A licitante responde pela fidelidade e legitimidade das informações prestadas (item 17.5).
(b) O Edital não prevê declaração do fabricante como documento obrigatório da proposta ou da habilitação, e o pedido de esclarecimento não é o instrumento para criar exigência não constante do instrumento convocatório. Fica ressalvada a faculdade de diligência (art. 64, inciso I, da Lei nº 14.133/2021), no prazo fixado pelo(a) Pregoeiro(a), sob pena de desclassificação (item 17.7 do Edital).
(c) O entendimento não está correto. O item 1.4.1 fala sobre proteção da CDN e não veda a existência de scrubbing centers na arquitetura da solução ofertada. A exigência é que cada ponto de presença disponha de capacidade de mitigação descentralizada e independente, com todas as funcionalidades de proteção, executando-se os mecanismos de proteção em camada de aplicação na própria borda (item 1.4.28). São admitidas soluções que possuam

scrubbing centers como componente complementar, inclusive para ataques volumétricos, desde que a mitigação exigida no item 1.4.1 não dependa do desvio de tráfego para infraestrutura apartada.

Atenciosamente,

PRESIDENTE E 1º PREGOEIRO DA COMISSÃO PERMANENTE DE CONTRATAÇÃO DO TJCE

Às empresas interessadas em participar do Pregão Eletrônico nº. 032/2026.