OFÍCIO N. 171/2026
ASSUNTO: Pedido de esclarecimentos ao Edital do PE nº. 032/2026.
PROCESSO N. 8515550-95.2025.8.06.0000

Fortaleza, 02 de setembro de 2026.

Prezado (s) Senhor (es),

Em resposta ao questionamento enviado ao endereço eletrônico da Comissão Permanente de Contratação do TJCE, em 31/08/2026 às 15:36h, por empresa interessada em participar do Pregão Eletrônico n. 032/2026, informo os esclarecimentos, que seguem:

Pergunta 1:

"1 – Dimensionamento de FQDNs/Aplicações
Referência: Dimensionamento do LOTE2: WAF
Questionamento: Para que seja possível realizar o correto dimensionamento arquitetural e a precificação exata da solução de WAF SaaS (Edge Security), solicitamos esclarecer: Qual é a quantidade exata ou confiavelmente estimada de FQDNs (Fully Qualified Domain Names) e/ou aplicações web que estarão sob o escopo de proteção das soluções de WAF contratadas neste edital?

Resposta 1:

O quantitativo está definido no item 1.4.15 do Anexo II – Especificações Técnicas – Lote 2 do Termo de Referência: a CONTRATADA deverá prover aceleração e proteção para, no mínimo, 255 (duzentos e cinquenta e cinco) FQDNs pertencentes ao TJCE, registrados sob 1 (um) domínio (tjce.jus.br). Este é o parâmetro objetivo a ser considerado pelas licitantes para o dimensionamento arquitetural e a precificação de suas propostas.

Pergunta 2:

"2 – Dimensionamento de Load Balancer
Referência: 1.4.25.1. Considerando que o TJCE possui dois links dedicados de internet com múltiplos endereços IP publicados, a solução de CDN deverá suportar configuração de múltiplos servidores de origem, permitindo balanceamento automático de carga, failover transparente entre links distintos e monitoramento contínuo de disponibilidade dos serviços;
Questionamento: Visando a precificação e a parametrização adequadas da solução de balanceamento de tráfego, questionamos: Qual o quantitativo exato de aplicações web (ou FQDNs) que exigirão a configuração de serviço de Load Balancer por parte da contratada?

Resposta 2:

A exigência do item 1.4.25.1 do Anexo II constitui requisito funcional da plataforma CDN/ WAF, e não serviço autônomo de balanceamento a ser contratado ou precificado por aplicação. O requisito aplica-se ao conjunto de FQDNs protegidos pela solução (item 1.4.15 –

mínimo de 255 FQDNs), no cenário descrito nos itens 1.4.25.1 a 1.4.25.3: dois links dedicados de internet, configuração de origem principal e origem backup (standby) e operação em modo ativo-passivo, com failover automático e retorno ao link prioritário, entre pelo menos 2 (dois) links de internet.

Pergunta 3:

"3 – Dimensionamento de Inspeção de Arquivos/Sandbox
Referência: 1.5.14. A solução de WAF deve possuir funcionalidade que inspecione arquivos que são enviados através de upload para as aplicações, usando funcionalidades como Antivírus, Sandbox e técnicas para bloqueio de Trojans/backdoors, assim como análise de informações em arquivos JSON.
Questionamento: Considerando que as soluções de proteção avançada contra malwares exigem volumetria para dimensionamento de infraestrutura, solicitamos informar: Quantas aplicações web deverão ser configuradas com recursos de inspeção contra vírus em arquivos recebidos (uploads) de usuários e utilização de sandbox? Adicionalmente, há uma estimativa de volume mensal (em Gigabytes e quantidade de arquivos) que passarão por essa inspeção?

Resposta 3:

A funcionalidade descrita no item 1.5.14 do Anexo II é requisito nativo da solução, a ser habilitado por política de segurança nas aplicações protegidas, conforme definição conjunta entre CONTRATANTE e CONTRATADA na fase de implantação (itens 1.9.10 a 1.9.12). O universo potencial de aplicação da funcionalidade é o mesmo estabelecido no item 1.4.15. O edital não estabelece volumetria segregada de arquivos ou de gigabytes para essa funcionalidade, e tal informação não constitui parâmetro de dimensionamento ou de aceitação de propostas neste certame. O dimensionamento da solução está vinculado à franquia mensal de 50 TB de tráfego inspecionado (Anexo II, Item 1, e item 1.3.5), acrescida da franquia adicional sob demanda (Anexo II, Item 2), cabendo à licitante dimensionar sua proposta com base nesses parâmetros objetivos.

Pergunta 4:

"4 – Dimensionamento de proteção e monitoramento contra scripts executados no lado do cliente
Referência: 1.8.19. A solução deverá monitorar scripts JavaScript executados no lado do cliente, identificando comportamentos suspeitos, tentativas de roubo de dados, web skimming, formjacking, alterações indevidas e comunicação com destinos não autorizados.
Questionamento: O modelo de licenciamento das melhores tecnologias de mercado para proteção de scripts no lado do cliente — que garantem a segurança de scripts JavaScript e mitigam ataques como web skimming (Magecart) e formjacking — é baseado no tráfego de usuários. Dessa forma, solicitamos esclarecer: (A) Qual o quantitativo de aplicações web que receberão essa proteção específica? (B) Qual é o Volume Mensal Estimado de Page Views (Visualizações de Página)?

Resposta 4:

O **Resposta**: (A) O universo de aplicações é o definido no item 1.4.15 do Anexo II, com habilitação da funcionalidade por política de segurança, conforme definição conjunta na fase de implantação (itens 1.9.10 a 1.9.12).

(B) O edital não adota modelo de licenciamento baseado em visualizações de página (page views). O modelo de contratação é por franquia mensal de tráfego inspecionado (50 TB/mês), acrescida de franquia adicional sob demanda (Anexo II, Itens 1 e 2). Registre-se que, nos termos do item 1.8.21, a solução deverá realizar análise em tempo real de 100% das sessões reais de usuários, não sendo admitida análise por amostragem (sampling). Eventual composição interna do licenciamento da tecnologia ofertada é ônus exclusivo da licitante, que deverá dimensionar sua proposta de modo a atender integralmente aos requisitos do edital durante toda a vigência contratual, sem custos adicionais para o TJCE.

Pergunta 5:

“**5 – Integrações de Ecossistema**
Referência: 4.10.3.3. Integração com a infraestrutura de rede, serviços de autenticação e sistemas de monitoramento já implantados, como SIEM e ferramentas de visibilidade do ambiente;
Questionamento: Para assegurar que a solução de segurança de borda proposta tenha total interoperabilidade e integração nativa com o centro de operações do órgão, questionamos: Quais são as ferramentas (fabricantes e versões) atuais de SIEM, Monitoração, ITSM e Automação utilizadas pelo órgão? Existem requisitos técnicos ou protocolos específicos exigidos para a exportação de logs e integração sistêmica com essas ferramentas?

Resposta 5:

O item 4.10.3.3 do Termo de Referência refere-se expressamente ao Lote 1 – Controlador de Entrega de Aplicações (ADC). Para o Lote 2 – WAF como Serviço (SaaS), aplica-se o item 4.10.4.2, que exige integração via APIs e protocolos padrão para troca de informações com as plataformas internas do TJCE.
A exigência editalícia limita-se, portanto, ao suporte de armazenamento e exportação de logs para fontes externas (item 1.4.55 do Anexo II) por meio de formatos e protocolos abertos e amplamente utilizados no mercado. Por razões de segurança institucional, o TJCE não divulga, em sede de esclarecimento, os fabricantes e as versões de suas ferramentas internas de segurança, monitoramento e gestão de serviços. Tais informações serão fornecidas à CONTRATADA na fase de implantação, observado o dever de sigilo e confidencialidade previsto no edital.

Pergunta 6:

“**6 – Divergência em Carga Horária de Treinamento**
Referências: 3. ITEM 3 – TREINAMENTO – 3.6. O treinamento deverá ter carga horária mínima de 24 (vinte e quatro) horas, distribuídas conforme aprovado pelo CONTRATANTE.

1.11. DAS CARACTERÍSTICAS DO TREINAMENTO – 1.11.6. O treinamento terá carga horária mínima de 20 (vinte) horas, ministrada de forma a abranger integralmente o conteúdo previsto neste contrato, com limite de até 4 (quatro) horas diárias.
Questionamento: Nota-se uma incongruência na documentação técnica referente aos treinamentos.
A especificação do Lote 2 prevê a exigência mínima de 20 horas de treinamento (para até 8 participantes), contudo, a visão geral do Termo de Referência (TR) estipula 24 horas. Para fins de correta elaboração de proposta técnica e comercial, solicitamos esclarecer: Qual é a carga horária definitiva a ser exigida?

Resposta 6:

Não há divergência. O item 3.6 (carga horária mínima de 24 horas) integra o Anexo I – Especificações Técnicas – Lote 1 e refere-se ao treinamento oficial da solução ADC – Controlador de Entrega de Aplicações (v. itens 3.1 e 3.5 do mesmo Anexo). O item 1.11.6 (carga horária mínima de 20 horas) integra o Anexo II – Especificações Técnicas – Lote 2 e refere-se ao treinamento da solução WAF.
Para o Lote 2 – WAF, portanto, aplica-se a carga horária mínima de 20 (vinte) horas, com limite de até 4 (quatro) horas diárias, para turma composta por até 8 (oito) participantes da equipe técnica do TJCE, nos termos dos itens 1.11.6 e 1.11.7 do Anexo II.

Pergunta 7:

“**7 – Estratégia de Mitigação DDoS e Scrubbing Centers**
Referência: 1.4.1. A CDN deve possuir e disponibilizar no mínimo 2 (dois) pontos de presença (PoP) nacional e 50 (cinquenta) fora do Brasil, cada um com capacidade de mitigação descentralizada e independente, com todas as funcionalidades de proteção (sem a necessidade de desvio de tráfego para um “scrubbing center”), com capacidade de mitigação total da rede, nacional e internacional, de 100 (cem) Terabits por segundo (Tbps).
Questionamento: O item 1.4.1 determina que a mitigação deve ocorrer sem a necessidade de desvio para "scrubbing centers". Contudo, tecnicamente, o uso de Scrubbing Centers (centros de depuração dedicados de altíssima capacidade) é uma das estratégias arquiteturais mais avançadas e robustas adotadas globalmente pelas maiores empresas de CDN e segurança. Essa estratégia evita gargalos na rede principal, isolando volumes massivos de tráfego malicioso em infraestruturas especializadas e gerando uma melhora drástica e significativa na disponibilidade e performance do tráfego legítimo entregue. Visando garantir o acesso às melhores tecnologias de mercado e a máxima resiliência para o órgão, entende-se e confirma-se que serão aceitas soluções de CDN/WAF que utilizem a arquitetura de Scrubbing Centers para tratativa de tráfego em cenários de ataques volumétricos?

Resposta 7:

O entendimento está parcialmente correto. Permanece mantida a exigência prevista no item 1.4.1 do Anexo II, segundo a qual cada ponto de presença (PoP) deve possuir capacidade de mitigação descentralizada e independente, com todas as funcionalidades de proteção, sem a necessidade de desvio de tráfego para scrubbing center, visto que o objeto deste item contempla a proteção do tráfego HTTP/HTTPS das aplicações publicadas na plataforma, a

ser executada na própria borda (edge), de forma integrada às funções de CDN e WAF (item 1.4.28).
Ressalta-se que o edital não impede que a solução utilize scrubbing centers como componente complementar de sua arquitetura, especialmente em estratégias de mitigação de ataques DDoS volumétricos. A vedação existente refere-se exclusivamente à dependência de desvio de tráfego para infraestrutura externa para a execução das funcionalidades de proteção exigidas(item 1.6.6).

Pergunta 8:

“8 – Emissão e Gestão de Certificados Digitais
Referências: 1.4.24.8. A solução deverá suportar a gestão automática de certificados digitais gerados na solução, incluindo renovação, com integração nativa, no mínimo, ao serviço Let’s Encrypt, sem custos adicionais de licenciamento para o TJCE;
Questionamento: O edital exige que a contratada realize a emissão e a gestão automática (com integração ao Let's Encrypt, incluindo renovações) de certificados digitais sem custos adicionais.
Para a correta segregação de responsabilidades e viabilidade técnica da arquitetura de proxy reverso (CDN/WAF), entende-se que esta exigência (emissão e gestão) se aplica única e exclusivamente aos certificados gerados *dentro da plataforma de WAF da Contratada* (certificados de borda/Edge, que validam a comunicação entre o usuário e a CDN). Os demais certificados vinculados diretamente às instâncias das aplicações web (servidores de origem do cliente) deverão continuar sendo providenciados e tratados pelo próprio órgão de TI. O entendimento está correto?

Resposta 8:

O entendimento está correto. A exigência de gestão automática prevista no item 1.4.24.8 do Anexo II alcança os certificados digitais gerados na própria plataforma da CONTRATADA (certificados de borda/edge, que asseguram a comunicação entre o usuário final e a CDN), incluindo emissão e renovação, com integração nativa, no mínimo, ao serviço Let’s Encrypt, sem custos adicionais para o TJCE. Permanecem igualmente aplicáveis os itens 1.4.22 e 1.4.23, inclusive quanto à obtenção da qualificação “A” na ferramenta SSL Labs para todas as URLs publicadas na CDN.
Os certificados digitais vinculados diretamente aos servidores de origem das aplicações permanecem sob responsabilidade do TJCE.

Pergunta 9:

“9 – Limite de Inspeção de Corpo de Requisição HTTP/HTTPS
Referência: 1.4.30. A CDN deverá realizar inspeção completa de corpo de requisições HTTP/HTTPS, sem limitação de tamanho.
Questionamento: O edital requer inspeção completa do corpo de requisições "sem limitação de tamanho". Tecnologicamente e de acordo com as melhores práticas globais de segurança cibernética, realizar a inspeção ilimitada de payload (Deep Body Inspection) degrada severamente a latência e a performance da aplicação sem trazer ganhos de segurança. O padrão consolidado no mercado estabelece que a inspeção de pacotes com tamanho de até 32KB é o suficiente e o ideal para abranger a média

máxima de payload legítimo e detectar parâmetros e assinaturas maliciosas em aplicações web. O órgão confirma o entendimento de que a inspeção do corpo da requisição pelo WAF com limite de até 32KB atende plenamente à exigência, garantindo o equilíbrio ideal entre máxima proteção e alta performance para a aplicação?

Resposta 9:

O entendimento está parcialmente correto. A expressão “sem limitação de tamanho”, constante do item 1.4.30 do Anexo II, não impõe capacidade física ilimitada de inspeção; veda que a inspeção do corpo das requisições HTTP/HTTPS seja restringida por plano, licença, módulo adicional, nível de serviço ou política comercial da CONTRATADA, nos termos dos itens 1.3.6 e 1.3.7 do Anexo II — este último expresso quanto às técnicas de inspeção profunda de pacotes (DPI).

Atenciosamente,

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

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